Case No. 22-15961

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

DONALD J. TRUMP, the Forty-Fifth President of the United States; LINDA CUADROS; AMERICAN CONSERVATIVE UNION; RAFAEL BARBOSA; DOMINICK LATELLA; WAYNE ALLYN ROOT; NAOMI WOLF,
Plaintiffs-Appellants,

v.

TWITTER, INC.; JACK DORSEY,
Defendants-Appellees,

and

UNITED STATES OF AMERICA,
Intervenor-Appellee.

Appeal from the United States District Court for the Northern District of California (San Francisco), Case No. 3:21-cv-08378-JD · The Honorable James Donato, District Judge

EXCERPTS OF RECORD
VOLUME II OF III – Pages 59 to 153

JOHN P. COALE
2901 Fessenden Street NW
Washington, D.C. 20008
Telephone: (202) 255-2096
johnpcoale@aol.com

ALEX KOZINSKI
719 Yarmouth Road, Suite 101
Palos Verdes Estates, CA 90274
Telephone: (310) 541-5885
alex@kozinski.com

ANDREI POPOVICI
MARIE L. FIALA
LAW OFFICE OF ANDREI D. POPOVICI, P.C.
2121 North California Blvd., Suite 290
Walnut Creek, CA 94596
Telephone: (650) 530-9989
andrei@apatent.com
marie@apatent.com

Attorneys for Plaintiffs-Appellants,
Donald J. Trump, the Forty-fifth President of the United States;
Linda Cuadros; American Conservative Union; Rafael Barbosa;
Dominick Latella; Wayne Allyn Root

COUNSEL PRESS · (213) 680-2300 PRINTED ON RECYCLED PAPER

JOHN P. COALE *(pro hac vice)*
2901 Fessenden Street NW
Washington, DC 20008
Telephone: (202) 255-2096
Email: johnpcoale@aol.com

JOHN Q. KELLY *(pro hac vice)*
MICHAEL J. JONES *(pro hac vice)*
RYAN TOUGIAS *(pro hac vice)*
IVEY, BARNUM & O'MARA, LLC
170 Mason Street
Greenwich, CT 06830
Telephone: (203) 661-6000
Email: jqkelly@ibolaw.com
Email: mjones@ibolaw.com

FRANK C. DUDENHEFER , JR. *(pro hac vice)*
THE DUDENHEFER LAW FIRM L.L.C.
2721 Saint Charles Avenue, Suite 2A
New Orleans, LA 70130
Telephone: (504) 616-5226
Email: fcdlaw@aol.com

ANDREI POPOVICI (234820)
MARIE FIALA (79676)
LAW OFFICE OF ANDREI D. POPOVICI, P.C.
2121 North California Blvd. #290
Walnut Creek, CA 94596
Telephone: (650) 530-9989
Facsimile: (650) 530-9990
Email: andrei@apatent.com
Email: marie@apatent.com

RICHARD POLK LAWSON (*pro hac vice*)
GARDNER BREWER MARTINEZ MONFORT
400 North Ashley Drive
Suite 1100
Tampa, FL 33602
Telephone: (813) 221-9600
Facsimile: (813) 221-9611
Email: rlawson@gbmmlaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

DONALD J. TRUMP, the Forty-Fifth President of the United States, LINDA CUADROS, AMERICAN CONSERVATIVE UNION, RAFAEL BARBOZA, DOMINICK LATELLA, WAYNE ALLYN ROOT, NAOMI WOLF, INDIVIDUALLY, AND ON BEHALF OF THOSE SIMILARLY SITUATED,

Plaintiffs,

v.

TWITTER, INC., and JACK DORSEY,

Defendants

Case No: 3:21-cv-08378-JD

DECLARATION OF RICHARD P. LAWSON IN SUPPORT OF PLAINTIFF'S REPLY TO THE DEFENDANT'S OPOSITION TO THE MOTION FOR PRELIMINARY INJUNCTION

Hearing Date: February 24, 2022
Courtroom: 11, 19th Floor
Time: 10:00 a.m.
Judge: Hon. James Donato

DECLARATION OF RICHARD P. LAWSON

I, Richard P. Lawson, declare as follows:

1. I am an attorney admitted to practice *pro hoc vice* before this Court and am a member in good standing with the Florida Bar. I am a partner at the law firm of Gardner, Brewer, Hudson, P.A., counsel for the Plaintiffs in this action. I make this Declaration based on my own personal knowledge. If called as a witness, I could and would testify as follows.

2. Plaintiffs have filed a motion for preliminary injunction ("Motion").

3. This Declaration is being filed in support of Plaintiffs' Reply ("Reply") to the Defendants' opposition to the Motion ("Opposition").

4. This Declaration sets forth the basis for several factual references made in the Reply.

5. The former president of the Internet Association, Michael Beckerman, stated that Section 230 is, "the one line of federal code that has created more economic value in this country than any other." A copy of an article from National Public Radio quoting Mr. Beckerman can be found at **Exhibit A**.

6. David Post, former Temple University law professor and current Adjunct Scholar at the Cato Institute stated that the potential liability facing social media companies without Section 230 would have been "astronomical" and that it is unlikely that, "an investor [would provide] funds for any of these ventures in a world without Section 230." A copy of his opinion article from the Washington Post, "A bit of Internet history, or how two members of Congress helped create a trillion or so dollars of value," can be found at **Exhibit B.**

7. It has been estimated that the Congressionally mandated safe harbors of Section 230 and the Digital Millennium Copyright combine together to provide more than $40 billion dollars a year of value to the technology industry. A copy of a 2017 report from the Internet Association detailing the value of these safe harbors can be found at **Exhibit C.**

8. Since enactment of Section 230, growth in value of internet related companies has grown nine-fold. A copy of a chart from the Bureau of Economic Analysis detailing this growth can be found at **Exhibit D**.

9. On January 10, 2022, I visited the online edition of the *The Wall Street Journal* and retrieved the stock and market data for Alphabet, Meta Platforms, and Twitter, copies of which can be found at **Exhibits E, F, and G, respectively**.

10. SEC Form 10-K reports for the year ending December 31, 2020 for Alphabet, Meta Platforms, and Twitter can be found at **Exhibits H, I, and J, respectively**.

I hereby declare under the laws of the State of Florida and the United States of America that the foregoing is true and accurate and that this declaration was executed on January 10, 2022, in Tampa, Florida.

By: */s/ Richard P. Lawson*
Richard P. Lawson

Exhibit A

All Tech Considered

THE NEW CLASH BETWEEN FREE SPEECH AND PRIVACY

Section 230: A Key Legal Shield For Facebook, Google Is About To Change

March 21, 2018 · 5:11 AM ET
Heard on Morning Edition

ALINA SELYUKH

7-Minute Listen

PLAYLIST Download Transcript

A 1996 law sits at the heart of a major question about the modern Internet: How much responsibility should fall to online platforms for how their users act and get treated?

Oivind Hovland/Getty Images/Ikon Images

Updated at 5:17 p.m. ET

It's 1995, and Chris Cox is on a plane reading a newspaper. One article about a recent court decision catches his eye. This moment, in a way, ends up changing his life — and, to this day, it continues to change ours.

The case that caught the congressman's attention involved some posts on a bulletin board — the early-Internet precursor to today's social media. The ruling led to a new law, co-authored by Cox and often called simply "Section 230."

This 1996 statute became known as "a core pillar of Internet freedom" and "the law that gave us modern Internet" — a critical component of free speech online. But the journey of Section 230 runs through some of the darkest corners of the Web. Most egregiously, the law has been used to defend Backpage.com, a website featuring ads for sex with children forced into prostitution.

Today, this law still sits at the heart of a major question about the modern Internet: *How much responsibility do online platforms have for how their users behave or get treated?*

In the first major change to Section 230 in years, Congress voted this week to make

Internet companies take a little more responsibility than they have for content on their sites.

Library or newspaper?

The court decision that started it all had to do with some online posts about a company called Stratton Oakmont. On one finance-themed bulletin board, someone had accused the investment firm of fraud.

Years later, Stratton Oakmont's crimes would be turned into a Hollywood film, *The Wolf of Wall Street*. But in 1994, the firm called the accusations libel and wanted to sue. But because it was the Internet, the posts were anonymous. So instead, the firm sued Prodigy, the online service that hosted the bulletin board.

Prodigy argued it couldn't be responsible for a user's post — like a library, it could not liable for what's inside its books. Or, in now-familiar terms: It's a platform, not a publisher.

POLITICS

Congress Passes Legislation To Curb Online Sex Trafficking Of Children

LISTEN · 4:12 PLAYLIST Download Transcript

SUBSCRIBE TO PODCAST

The court disagreed, but for an unexpected reason: Prodigy moderated posts, cleaning up foul language. And because of that, the court treated Prodigy like a newspaper liable for its articles.

As Cox read about this ruling, he thought this was "exactly the wrong result": How was this amazing new thing — the Internet — going to blossom, if companies got punished for *trying* to keep things clean? "This struck me as a way to make the Internet a cesspool," he says.

At this moment, Cox was flying from his home in California to return to Congress. Back at work, Cox, a Republican, teamed up with his friend, Oregon Democrat Ron Wyden, to rectify the court precedent.

Together, they produced Section 230 — perhaps the only 20-year-old statute to be claimed by Internet companies and advocates as technologically prescient.

Sen. Ron Wyden, D-Ore., (left) and Rep. Christopher Cox, R-Calif., speak about the Communications Decency Act in 1997.

They were behind Section 230, which says that with some exceptions, online platforms can't be sued for something posted by a user.

Douglas Graham/Congressional Quarterly/Getty Images

"The original purpose"

Section 230 lives inside the Communications Decency Act of 1996, and it gives websites broad legal immunity: With some exceptions, online platforms can't be sued for something posted by a user — and that remains true even if they act a little like publishers, by moderating posts or setting specific standards.

"Section 230 is as important as the First Amendment to protecting free speech online, certainly here in the U.S.," says Emma Llanso, a free expression advocate at the Center for Democracy and Technology.

> "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> 47 U.S. Code § 230

The argument goes that without Section 230, we would never have platforms like YouTube, Facebook, Twitter, Yelp or Reddit — sites that allow ordinary people to post opinions or write reviews.

It's "the one line of federal code that has created more economic value in this country than any other," says Michael Beckerman, who runs the Internet Association, which represents many of Silicon Valley's largest companies.

But Section 230 is also tied to some of the worst stuff on the Internet, protecting sites when they host revenge porn, extremely gruesome videos or violent death threats. The

broad leeway given to Internet companies represents "power without responsibility," Georgetown University law professor Rebecca Tushnet wrote in an oft-cited paper.

Cox says, "The original purpose of this law was to help clean up the Internet, not to facilitate people doing bad things on the Internet."

"A Teflon shield"

The original purpose hasn't always prevailed in court. And one specific example has prompted Congress to vote to amend Section 230 — the first cutback to websites' protections in years.

It's the case of Backpage.com, a site ostensibly for classifieds, but one well known for its adult-services ads. Among them — if you know what to look for — are sex ads featuring children forced into prostitution.

THE TWO-WAY

Backpage Shuts Down Adult Ads In The U.S., Citing Government Pressure

"All of those terms were indicative of an underage child — Lolita, fresh, new to town," says Mary Mazzio, a filmmaker whose documentary I Am Jane Doe tells the story of several young girls sold for sex on Backpage.

Over the years, victims and their families brought case after case against Backpage — and lost. The website kept convincing judges across the country that Section 230 shielded it from liability for the posts of its users. Major digital-rights groups, including the Center for Democracy and Technology, argued that holding Backpage liable could have chilling effects for social media and other websites.

This bewildered Mazzio: "How is it possibly legal that a website that makes millions and millions of dollars has no accountability for this crime?" she says. "Section 230

has turned into a Teflon shield, not to protect free speech but to protect business revenue."

The Supreme Court last year declined to hear victims' appeal in the case of Backpage and Section 230.

Kubiiki P. wipes tears as she testifies at a 2017 Senate hearing about her young daughter being sold for sex on Backpage.com. The site, ostensibly for classifieds, is well-known for its adult-services ads.

Cliff Owen/AP

"The judge-made law"

Eventually, mounting evidence showed that Backpage was actively involved in the sex ads. That means the site is a publisher liable for its content. Backpage and its founders are now facing a federal grand jury in Arizona.

To Sen. Ron Wyden, co-author of the law, the Department of Justice missed the mark for not going after Backpage earlier, since Section 230 does not preclude federal criminal investigations.

Beyond Backpage, similar concerns continue to play out with sites that solicit revenge porn, publicly acknowledge potential risks to users or ignore harassment complaints.

"I'm afraid ... the judge-made law has drifted away from the original purpose of the statute," says Cox, who is now president of Morgan Lewis Consulting. He says he was shocked to learn how many Section 230 rulings have cited other rulings instead of the actual statute, stretching the law.

Cox argues that websites that are "involved in soliciting" unlawful materials or "connected to unlawful activity" should not be immune under Section 230. Congress should revisit the law, he says, and "make the statute longer and make it crystal clear."

Backpage.com executives — CEO Carl Ferrer (from left), former owner James Larkin, Chief Operating Officer Andrew Padilla, former owner Michael Lacey — are sworn in to testify before a Senate Homeland Security and Governmental Affairs subcommittee on investigations in January 2017.

Cliff Owen/AP

Responsibility

Cox draws this distinction of websites like Backpage — *involved* or *connected* with their content — and sites that are "pure intermediaries." He wouldn't say whether that term applied to Facebook or Google.

Interestingly, the Internet giants themselves — as well as Wyden — talk about the law as being rooted in responsibility.

"The real key to Section 230," Wyden says, "was making sure that companies in return for that protection — that they wouldn't be sued indiscriminately — were being responsible in terms of policing their platforms."

Beckerman of the Internet Association describes Section 230 as "not a blanket amnesty" but a call for responsible policing of platforms. The Internet companies say that on sex trafficking, they actively help investigate cases — and that generally, without Section 230, websites would resort to more censorship or decide to know as little as possible about what happens on their platforms.

But Danielle Citron, a University of Maryland law professor who authored the book *Hate Crimes in Cyberspace*, argues that responsibility is exactly what is missing from the law.

"Yes, let's think about the consequences for speech," she says, pointing to the flip side of the freewheeling Internet. "There are countless individuals who are chased offline as a result of cyber mobs and harassment."

People rally in 2014 at the Washington state Supreme Court, which heard a case filed by three victims of sex trafficking against Backpage.com, saying the website helped promote the exploitation of children.

Rachel La Corte/AP

A rift among companies

Politically, the story of Section 230 has recently taken a surprising turn.

The Backpage saga has galvanized lawmakers to act on bills amending Section 230 with the goal of stemming online sex trafficking. The legislation allows more state and civil lawsuits against websites related to online sex trafficking, for "knowingly assisting, supporting or facilitating" crimes.

The Senate passed the bill Wednesday, sending it to President Trump for his signature. The White House has supported the legislation.

And for the first time, after years of staunch defiance, the Internet Association came out in support of legislation to change Section 230, shocking smaller Internet companies and digital-rights groups by breaking ranks.

The industry giants are narrowly threading the needle. After the bill passed the House, the Internet Association said the industry not only is "committed to ending trafficking online" but also "will defend against attempts to weaken these crucial protections" of Section 230.

"We all share the same goal," the association's Beckerman told NPR, "and that's to ensure that victims are able to have justice they need, but also enable our companies to stop this practice."

POLITICS

House Passes Bill To Crack Down On Online Sex Trafficking

LISTEN · 2:46 PLAYLIST Download Transcript

SUBSCRIBE TO PODCAST

Engine, a group advocating on behalf of smaller Internet companies, argues that Silicon Valley behemoths like Google, Facebook and Twitter can handle more lawsuits and the legal uncertainty that would smother a startup.

Not the last challenge

Wyden points out that these are the very same platforms facing massive scrutiny for being manipulated by Russian operatives during the 2016 election, making it a politically touchy moment for the companies to fight over sex-trafficking legislation.

"The big companies have a lot of egg on their face over the election, and nobody wants to be seen as being soft on sex trafficking," he says.

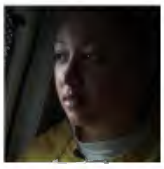
Wyden and Cox have opposed the legislation to amend Section 230, along with groups including Engine and the Center for Democracy and Technology. Opponents of the bill say it could lead to crimes moving deeper into the dark web and to websites resorting to more censorship or ignorance of what happens on their platforms to avoid liability.

Sen. Rob Portman, R-Ohio, author of the Senate bill, says the tech community "overreacted" to amending Section 230 "to the point that they weren't willing to look at the obvious problem, which is that it's been abused to sell people online."

Wyden says all this should be a wake-up call for Silicon Valley:

"If the technology companies do not wake up to their responsibilities — and use the power 230 gives them — to better protect the public against sex trafficking and countries that try to hack our political system, you bet that companies can expect (this legislation) will not be the last challenge for them."

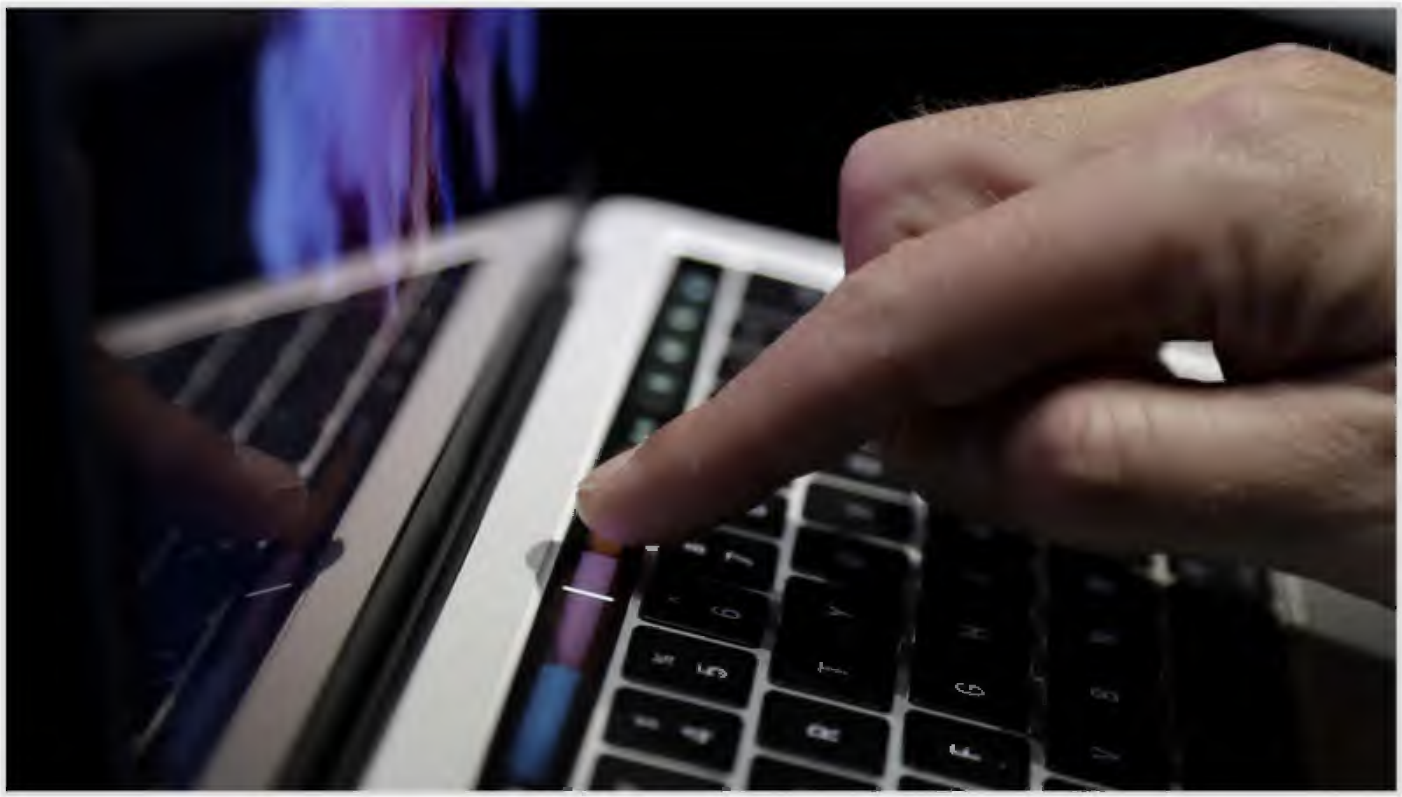
NPR researcher Will Chase and Business Desk intern Ian Wren contributed to this report.



HERE & NOW COMPASS

Cyntoia Brown Case Highlights How Child Sex Trafficking Victims Are Prosecuted

More Stories From NPR



TECHNOLOGY

The 'All Tech Considered' Blog Logs Off

TECHNOLOGY

One Woman's Facebook Success Story: A Support Group For 1.7 Million

POLITICS

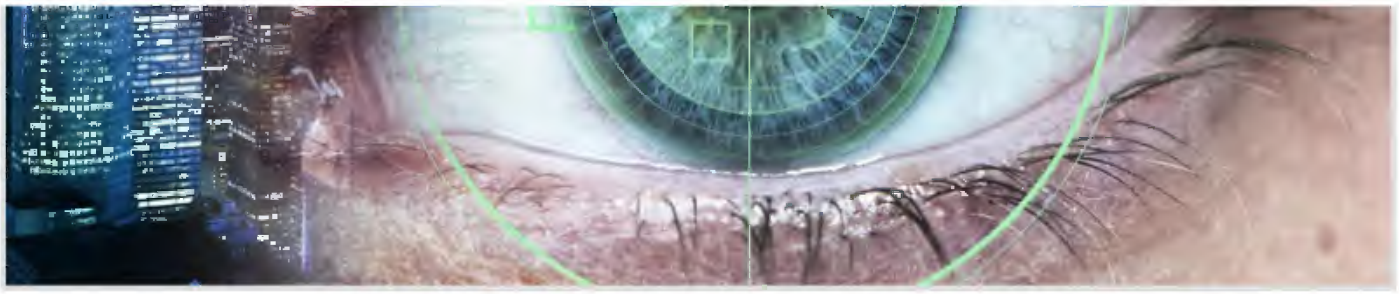
Inspired By Russia, He Bought Influence On Facebook

TECHNOLOGY

Do Not Sell My Personal Information: California Eyes Data Privacy Measure

ARTS & LIFE

Reading The Game: The Long Dark



TECHNOLOGY

3 Things You Should Know About Europe's Sweeping New Data Privacy Law

Popular on NPR.org

ASIA

Turkmenistan's leader wants 'Gates of Hell' fire put out

GLOBAL HEALTH

What we know about the symptoms — and the severity — of the omicron variant

GLOBAL HEALTH

A Texas team comes up with a COVID vaccine that could be a global game changer

OBITUARIES

Actor and comedian Bob Saget dies at 65

HEALTH

A guide to COVID tests: When to test, what kind to use and what your results mean

ELECTIONS

Congress may change this arcane law to avoid another Jan. 6

NPR Editors' Picks

EUROPE

U.S. and Russian diplomats meet, hoping to defuse tensions over Ukraine

ASIA

Myanmar's Suu Kyi sentenced to 4 more years in prison

RELIGION

On COVID vaccinations, Pope says health care is a 'moral obligation'

BOOK REVIEWS

In 'Wahala,' intimacy at times morphs into enmity

HEALTH

CDC is criticized for failing to communicate, promises to do better

POP CULTURE

Sidney Poitier was far more than just a symbol of racial progress

All Tech Considered

READ & LISTEN

Home

News

Arts & Life

Music

Podcasts & Shows

CONNECT

Newsletters

Facebook

Twitter

Instagram

Press

Contact & Help

ABOUT NPR

Overview

Diversity

Ethics

Finances

Public Editor

Corrections

GET INVOLVED

Support Public Radio

Sponsor NPR

NPR Careers

NPR Shop

NPR Events

NPR Extra

Exhibit C

NERA
ECONOMIC CONSULTING

5 June 2017

Economic Value of Internet Intermediaries and the Role of Liability Protections

By **Christian M. Dippon, PhD**

Summary

The U.S. Internet sector is one of our nation's most dynamic and successful economic performers, doubling its share of the U.S. economy between 2007 and 2014. The sector is driven by Internet intermediaries—companies that connect third parties on the Internet. Many of the Internet intermediaries are among the best known companies in the world, such as Amazon, Facebook, and Google. The rapid growth of these companies and the benefits consumers have gained from their presence have been aided by the availability of what are called Internet "safe harbors." These legal provisions protect Internet intermediaries and others that publish third-party content from being responsible for that content. The principal Internet safe harbors are found in the Communications Decency Act of 1996 and the Digital Millennium Copyright Act (DMCA) of 1998.

The robustness of these safe harbors is continually being challenged in the United States through legislative proposals and litigation. This litigation, originating either in the United States or abroad, has the result of exposing U.S. Internet intermediaries to very large legal liabilities. The legislative proposals have the potential to do the same. Additionally, the U.S. safe harbors are affected by the consequences of litigation or regulation elsewhere in the world, for example, from Europe's "Right to be Forgotten" enforcement.

We have estimated the economic costs of weakening the protections offered by Internet safe harbors as a consequence of legislation or litigation on the U.S. economy by surveying consumers in two areas: first in their use of Internet search engines and second in their use of cloud storage. The surveys measured the decline in consumer demand following an increase in price (in the case of cloud storage) or an increase in the number of advertisements (in the case of Internet search). The results of these surveys were then combined with a study measuring the overall economic contribution of the Internet sector to the U.S. economy to estimate the cost in terms of gross economic output, income, and employment in the United States following a weakening of Internet safe harbors.

Insight in Economics™

The consumer surveys reveal that increases in price for cloud storage and amount of advertising for Internet search will likely reduce revenues obtained by these two services by approximately 7.8 percent. This translates into a loss of over 53,000 jobs. Many of these jobs pay above average wages. Consequently, U.S. gross domestic product (GDP) would decrease by $5 billion annually for the search and cloud services categories alone.

There are many more Internet intermediaries (other than search and cloud services), and a weakening of safe harbor protections would affect most of them. Based on our findings, we estimate that the decline in the U.S. Internet sector would eliminate over 425,000 jobs. The U.S. gross domestic product would decrease by $44 billion annually.

In addition to these more easily measurable direct effects on the U.S. economy, a reduction in safe harbor protections will also have negative secondary effects. In particular, it will reduce the formation of Internet intermediary startups, as well as decrease investment in the Internet more generally.

Introduction

The Internet Association has asked me to measure the potential costs to the U.S. economy if the current safe harbor protections the industry operates under are reduced, in particular, the legislative safe harbors. It is important to note that this study focuses on just two of the many so-called verticals available to consumers (i.e., cloud storage and search services). Internet intermediaries also rely on the safe harbors to provide consumers with online travel booking, the sharing economy, and social media services, among others.

The U.S. economy has benefited tremendously from the growth of the U.S. Internet sector. The sector's success is partially attributable to specific legislation that protects Internet companies from legal prosecution over third-party content. Thus, it follows that a weakening of this legislation carries serious negative repercussions for the U.S. economy. This study assumes that the general structure of a market with safe harbors would remain in place but that changes due to legislation (e.g., mandatory filtering) or litigation (e.g., increased rejection of affirmative DMCA defenses) would weaken the safe harbors and significantly raise the costs of operating as an Internet intermediary, costs that would be borne by consumers. The objective of this study to ascertain the potential impact on the U.S. economy if current legislative protections, safe harbors in particular, are reduced through legislation or litigation. As part of this, we estimate how much Internet intermediaries might be forced to raise prices if safe harbor protections are reduced. We note that although this study focuses primarily on two consumer services protected by safe harbors (i.e., cloud storage and search), we also estimate an effect for overall Internet intermediaries because Internet intermediaries also rely on safe harbors to provide consumers with additional services, among others, with online travel booking, the sharing economy, and social media services.

Internet intermediaries provide platforms for the exchange of information, goods, and services. In addition, Internet intermediaries provide Internet access. According to the Organisation for Economic Co-operation and Development (OECD):

> Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.[1]

Examples of Internet intermediaries include some of the most well-known firms in the United States, including Google (operating as Alphabet), Facebook, Amazon, and eBay. It also includes more recent Internet companies such as Airbnb and Uber, as well as less consumer-facing firms such as Dropbox and Salesforce. There are, of course, many more such firms, and new ones are continually entering the marketplace.

Internet intermediaries are financed in a number of ways. Many of their services (e.g., Internet search) are paid for through digital advertising and are free to consumers. Other services (e.g., Internet access or cloud storage) are financed through retail revenue. The companies provide enormous consumer benefits by reducing search costs, transaction costs, and communications costs. For instance, there are an estimated 3.5 billion Google searches conducted worldwide per day.[2]

This paper is organized as follows. In Section III, we provide an overview of the safe harbor protections currently in place. Section IV describes some of the challenges to safe harbors. Section V addresses the importance of the Internet intermediaries to the U.S. economy. Section VI describes the survey methodology developed to estimate the impact of reducing safe harbor protections. In Section VII, we estimate the impact on the U.S. economy of the surveyed Internet intermediaries. Section VIII estimates the impact on the overall U.S. economy across all Internet intermediaries. Section IX concludes.

Overview of Safe Harbor Protections

In the United States, there are two main safe harbor protections for Internet intermediaries: the Communications Decency Act (CDA) of 1996 and the Digital Millennium Copyright Act (DMCA) of 1998.

The CDA, Section 230 in particular, was enacted in part to "promote the continued development of the Internet and other interactive computer services and other interactive media."[3] It does so by protecting Internet intermediaries such as Internet Service Providers (ISPs) and other online services that publish third-party content from being legally responsible for that content. The relevant paragraph states:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[4]

This bright-line rule has allowed user-generated Internet services like YouTube, Yelp, Reddit, and Facebook to flourish by facilitating consumer access through their ISPs.

The DMCA was enacted to update U.S. copyright laws. Section 512 of the DMCA was designed, in part, to deal with concerns that "without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet."[5] To alleviate Internet intermediary concerns, Congress created four safe harbors limiting copyright liability. These were for:

a) Transitory Digital Network Communications—… transmitting, routing, or providing connections for material through a system or network controlled or operated by or for the service provider….
b) System Caching—… storage of material on a system or network controlled or operated by or for the service provider….
c) Information Residing on Systems or Networks at Direction of Users—… storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider….
d) Information Location Tools—… referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link….[6]

Safe harbors do not provide blanket protection to ISPs and other intermediaries. In order to be protected under the four safe harbor provisions within the DMCA, an Internet intermediary satisfies the limitations of liability only if it "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[7]

The United States' success in developing the Internet intermediaries sector confirms the legislative reasoning behind the enactment of both the CDA and the DMCA. Industry observers generally indicate that an important reason for the success of U.S. intermediaries on a global scale is due to the space for innovation and application created by these safe harbors. Consequently, any changes that would diminish the robustness of the safe harbors would injure the U.S. economy.

In contrast, the greater uncertainty surrounding safe harbors in Europe has been viewed as one of the limiting factors to Internet intermediary development there. As one observer noted regarding the European context:

> Despite the guarantees offered by the Directive on electronic commerce to businesses which host or passively transmit illegal content, intermediary internet service providers struggle with the legal uncertainty linked to fragmentation within the European Union of the applicable rules and practices which are possible, required or expected of them when they are aware of illegal content on their websites. Such fragmentation discourages those who wish to conduct business online, and hinders its development.[8]

Similarly, as the Internet Association stated in the European Union (EU) context:

> The EU was also quick to recognize the challenges facing the early Internet. The eCommerce directive introduced a similar notice-and-takedown framework to the U.S. system for most content. Since it was a directive that needed to be interpreted by (eventually) 28 EU member states it has resulted in some inconsistency of application that provided somewhat less certainty to Internet companies than the more bright line U.S. safe harbors.[9]

The effects of the greater certainty, among other reasons, contributed to the business success of U.S.-based Internet intermediaries. A number of the U.S. Internet participants are among the most successful and innovative firms in the world. In 2014, the United States accounted for 13 of the 21 largest Internet companies in the world and if China is excluded, 13 of the largest 16. According to a study measuring the U.S. Internet, the sector accounted for 6 percent of GDP in 2014. It has also grown rapidly relative to other industries; its GDP share grew by over 88 percent between 2007 and 2012. It is also a sector where employment has grown rapidly, by almost 16 percent yearly between 2007 and 2012. Importantly, it is a sector with higher wages than the U.S. average, those employed in it earned almost 30 percent more on average in 2012.[10] Thus, U.S. Internet safe harbors function as an important catalyst to the U.S. economy.

Challenges to Safe Harbors

In the United States, there have been potential legislative interventions, as well as numerous lawsuits challenging the protection guaranteed by the safe harbors. The potential legislative interventions include proposals for mandatory content filtering, redefining what it means to "materially contribute" to the illegality of posted content, and enacting "Right to be Forgotten" laws. The lawsuits involve claims of damages that at times have been very large. For example, social media platforms have faced claims of providing material support to various terrorist groups in the form of access to their services, with at least one claim seeking $1 billion in compensatory damages.[11]

There have also been several successful lawsuits against Internet intermediaries that tested the legal limits of the safe harbors. In each case, significant damages were awarded against the intermediary involved. In 2014, BMG Rights Group, a music publishing company, sued Cox Communications, an ISP, for copyright infringement on 1,397 musical compositions across Cox's Internet service.[12] Despite Cox's assertion of the DMCA safe harbor as an affirmative defense, a jury found Cox "liable for willful contributory copyright infringement" for not taking appropriate steps to combat repeat infringers. In this case, BMG Rights Management was awarded $25 million in statutory damages.[13]

Another recent copyright infringement suit was filed against MP3tunes under the DMCA. In this case, the plaintiffs alleged that two Internet music services created by MP3tunes (MP3tunes.com and sideload.com) infringed on their sound recordings and musical compositions. One MP3tunes service operated as a locker service for storing digital music and the second allowed users to search for free music on the Internet and upload songs to the locker.[14] The locker storage service charged a fee to store the music on the MP3tunes server.[15] After the trial, which featured a safe harbor defense, the jury returned a verdict for the plaintiffs of $48 million, including $7.5 million in punitive damages against the owner of MP3tunes.[16] Statutory damages were allowed in lieu of actual damages up to $30,000 if MP3tunes acted innocently or up to $150,000 if it acted willfully.[17] The appeals court decision upheld the $41.5 million in damages, as well as the trial court reduction of the punitive damages award to $750,000.[18]

Challenges to intermediary safe harbors have not only occurred in the United States. In particular, there have been several successful ones in Europe, providing a window to the direction in which the United States could conceivably head. In May 2014, the European Court of Justice (ECJ) ruled:

> Individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them. This applies where the information is **inaccurate, inadequate, irrelevant or excessive**....[19]

This "Right to be Forgotten" decision applies to any search engine that is funded by selling advertising space. To reach this conclusion, the ECJ ruled: "Search engines are controllers of personal data."[20] According to *The New York Times*, in the year following this decision, Google received requests to "forget about a million web links" of which it removed about 40 percent.[21] Cases still exist where there is a dispute because Google did not remove the link. In the United Kingdom, people can appeal to the Information Commissioner's Office (ICO), which describes itself as an "independent body set up to uphold information rights."[22] The ICO will support either the search service or the complainant. If the search service disagrees with the ICO's request to delink the item, the search service could face legal action for noncompliance.[23] The first proposed law of its kind in the United States, which required that "search engines, publishers and similar online players remove information that individuals have identified as being 'inaccurate, irrelevant, inadequate or excessive' within 30 days," was introduced in the New York State Senate in February of this year.[24]

The "Right to be Forgotten" case was followed by *GS Media BV v. Sanoma Media Netherlands BV*, a September 2016 ECJ decision on the legality of linking to infringed materials, which found that merely linking (instead of copying) can lead to copyright liability. Although the decision acknowledged how difficult it would be for individuals or entities wanting to post a link to determine if the copyright holders allowed the posting, the court nonetheless imposed a duty to make that determination on those in "pursuit of financial gain," for example, an ad-supported website. Thus, according to an analysis published by *Law360*, the "court imposes a duty, for the first time, on whoever provides links to check the legitimacy of the linked material."[25] Specifically the court wrote:

> Furthermore, when the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead, so that it must be presumed that that posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder. In such circumstances, and in so far as that rebuttable presumption is not rebutted, the act of posting a hyperlink to a work which was illegally placed on the internet constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29.[26]

As the authors of the *Law360* piece note, the decision implicates any website with a European audience, and it "significantly increase[d] the risk of copyright infringement from linking to third-party material on a website or server that may not be operated by the copyright owner." The decision also leaves unclear what liability, if any, a social media platform operating for profit faces when its users link to websites that may be infringing.[27]

Although overall estimates of the possible litigation costs under a legislative regime offering fewer safe harbor protections are not currently available as far as we are aware, the numbers are potentially very large based on previous court decisions. For example, it has been noted that even the market for litigation funding (i.e., third-party investors funding litigation) in the United States reached an estimated $1 billion in 2010 and was expected to grow.[28]

Internet Intermediaries' Role in the Economy

Internet intermediaries such as eBay, Facebook, Google, IAC, Uber, and Yahoo! are a driving force of the modern U.S. economy. Numerous studies document the importance of these and many other entities both domestically as well as internationally. As referenced previously, a study titled "Measuring the U.S. Internet Sector" describes the growing importance of the Internet sector in detail. The study measures the economic contribution of "the provisioning of Internet backbone facilities, data storage, Internet access, Internet telephony, cloud computing, search activities, social media, Internet advertising, and E-Commerce."[29] It also compares the value added by the Internet sector in 2007 and 2012, as well as provides an estimate for 2014.[30] As can be seen in Table 1, during these periods, the Internet sector has more than doubled, growing at double digit annual rates.[31]

Table 1. **U.S. Internet Sector Growth Rates**

				Annual Growth Rate	
	2007	2012	2014	2007-12	2007-14
Value Added ($ billion)	$438.8	$847.5	$966.2	14%	12%
Direct Employment	1,383,633	2,873,009		16%	
Share of U.S. Economy	2.9%	5.5%	6.0%	14%	11%

Source: Siwek.

As the study explains, not only has direct employment in this sector grown rapidly, the sector also delivers higher per-employee earnings. In 2012, those directly employed in the Internet sector had an average compensation of $79,515 per year, an earnings premium of about 30 percent over the average compensation of all U.S. workers.[32]

The OECD, among others, has also made estimates of the value added contributed by the Internet sector. For a "narrow scope" estimate, which encompasses only the information services sector and the wholesale and retail sectors, it estimated the value added at 3.2 percent of the U.S. business sector value added in 2011. Measured at a "broader scope," which takes into account Internet-related activities across all industries in the business sector for which data are available, it estimated it as up to 13.8 percent of the U.S. business sector value added in 2011.[33] The OECD also notes the claim:

> There is a huge layer of the economy unseen in the official data, and for that matter, unaccounted for in the income statements and balance sheets of most companies. […] the trends in the official statistics not only underestimate our bounty, but in the second machine age they have also become increasingly misleading.[34]

An example would be the efficiency gains from a reduction in discovery costs an Internet user experiences through the ability to search or apps provided by a variety of Internet services. Another example is a "sharing economy" entity like Airbnb. While there was always residential rental business, the creation of an Internet platform like Airbnb, currently having a market capitalization similar to that of the largest hotel chains, has reduced entry barriers, increased market size, and minimized risks (for both the providers and the consumers of the services). It has done this by reducing search costs, increasing the use of the housing stock (e.g., apartments stay unused less frequently in their owners absence), and creating a greater range of prices for consumers to choose from.[35]

The benefits of the Internet intermediaries can be found not only in the domestic economy but also abroad as U.S. companies have "exported" their business models. For example, according to estimates from eMarketer, Facebook had worldwide advertising revenues of nearly $26 billion in 2016 of which 54 percent came from outside the United States.[36] Google had worldwide advertising revenues of over $63 billion of which 53 percent came from outside the United States.[37]

As this brief review shows, Internet intermediaries are crucial to both the U.S. domestic economy and U.S. exports to the rest of the world. In the following sections, we deal with the possible impact of putting limits on safe harbors; that is, limiting safe harbors would lead to a significant rise in the cost of providing access to Internet platforms to U.S. consumers. To estimate the impact on the U.S. economy, we combine consumer surveys regarding the impact of cost increases on two sectors of the Internet economy, search and consumer cloud storage.

Survey Methodologies

As shown above, potential litigation costs from a reduction in safe harbor protection can be significant and include not only claimed economic damages, but also legal fees and potential punitive claims. Consequently, a permanent weakening of Internet safe harbors exposes all Internet companies, large and small, to significant litigation expenses and expenses aimed at minimizing such suits in the first place.

To ensure that these costs will not cripple them, Internet intermediaries would need to increase their prices or their volume of advertising or both to cover the additional litigation-related expenses that would result from a reduction in safe harbor protections. Given that all Internet intermediaries would be impacted by the weakening of safe harbors, it is reasonable to assume that a large part of these additional costs would be passed on to end users. Naturally, an increase in price usually results in a decrease in demand. To measure the decrease in demand as a result of a price increase, we conducted two consumer surveys. The first survey measured a demand decrease for Internet search (e.g., fewer searches conducted), whereas the second survey measured the demand decrease for cloud storage. We note that these are only two of many services offered by Internet intermediaries and are meant to illustrate the impact of a reduction in safe harbor protection.

We assume that the essential structure of the two types of service which we surveyed would not change; that is, Internet search still would be free to the user. To estimate the drop in demand for Internet services due to an increase in price or the volume of advertising, we conducted two consumer surveys. One survey focused on demand for cloud storage services and the other focused on Internet search. Each survey was designed as a choice-based conjoint analysis, which is a statistical technique that allows market researchers to determine the value that consumers place on the features of a product or service. Choice-based conjoint analysis asks consumers to select their most preferred product from sets of hypothetical products made up of "bundles" of attributes. This survey approach is common in market and academic research and allows researchers to estimate how consumers value a particular attribute by observing how they make tradeoffs between the attributes of the various products they consider. In our study, we are interested in how consumers will balance consumption of a service (cloud storage or Internet searches) with an increased cost of the good (price or advertising). The details of each survey are provided below.

Cloud Storage

Cloud storage consists of services that allow a user to upload and store digital data in a remote server, which can then be accessed, edited, and shared via a cloud storage application such as iCloud or Dropbox. According to a 2013 survey, cloud storage is overwhelmingly used for music.[38] The cloud storage survey was administered to an online panel of 300 individuals. The survey was limited to individuals who stated that they used or were considering using a cloud storage service.

After qualifying for the survey, respondents were presented with descriptions of six attributes of cloud storage service plans they might consider when choosing a service. These attributes were (1) does the service automatically back up one or more devices, (2) are stored files encrypted, (3) are there options to allow others to view, download, or edit files, (4) what is the maximum size of an individual file that can be uploaded, (5) the monthly price of the service, and (6) the amount of monthly storage included in the plan. These attributes and the levels of each attribute were selected to reflect the characteristics of real-world cloud storage services. A detailed description of the attributes and the levels of these attributes are presented in Appendix A.

The survey respondents were asked to make a series of choices from sets of hypothetical cloud storage services. Each choice scenario shown to the respondents presented three hypothetical cloud storage services with a distinct combination of the six attributes described above. Respondents were asked to select the service they would be most likely to purchase or to state if they would not purchase any of the three services presented. An example of one choice scenario presented to respondents is shown in Table 2.

Table 2. **Example of a Choice Scenario in the Cloud Storage Conjoint Analysis**

Assuming that these three cloud data storage services are the only ones available to you, which cloud data storage service are you MOST likely to purchase? If you would not purchase any of these cloud data storage services, please select "I would not choose any of these services" below.

For additional information about each feature, hover your mouse over or tap the bolded words.

Scenario 2 of 12 *(Select one)*

	Plan 1	Plan 2	Plan 3
Automatic Backup	No	Multiple devices	One device
Encryption	No	Yes	Yes
File Sharing	View or download only	View, download, and real-time editing	No file sharing
Fite Size Restrictions	Unlimited	250 MB	2 GB
Price	$24.99	$1.99	$9.99
Storage	5 GB	1000 GB	100 GB
Your Choice	❑	❑	❑

❑ I would not choose any of these services

Each respondent was presented with 12 different choice scenarios in total, giving us a total of 3,600 choices from among these hypothetical cloud storage services.

We analyzed these choices with a conditional logit model, which allowed us to determine how each attribute influences the probability that an individual will purchase a cloud storage service.[39] The results were sensible; that is, a desire for more storage, larger file upload sizes, encryption, and the ability to back up multiple devices lead to higher probabilities of purchasing the service, whereas higher prices reduce the probability of purchasing the service. File sharing and the ability to only back up one device did not have a statistically significant effect on choice. The results of estimating this conditional logit model are presented in Table 3. These estimates are used to simulate the drop in demand from a hypothetical price increase in cloud storage services in the following section.

Table 3. **Conditional Logit Analysis of Cloud Storage Service Choices**

Attribute	Coefficient	Standard Error	Z-Score
Automatic Backup for One Device	-0.0588	0.0599	-0.98
Automatic Backup for Multiple Devices	0.5152	0.0478	10.77
Encryption	0.3662	0.0437	8.38
File Sharing: View or Download Only	0.0134	0.0545	0.25
File Sharing: View, Download, and Real-Time Editing	0.0597	0.0534	1.12
File Size Restrictions (TB)	0.0002	0.00001	2.99
Price	-0.0641	0.0027	-23.72
Storage (TB)	0.6942	0.0547	12.68

The market simulations to estimate the drop in cloud storage demand are discussed in Section C below.

Internet Search

The structure of the Internet search survey differs from that of the cloud storage survey—most Internet users would not opt out of Internet search and are unfamiliar with the concept of paying for it. Further, companies that provide Internet search have found it profitable to offer search for free and generate revenue through advertising. This means that the more standard approach of examining the tradeoff between price and demand for the service is unlikely to yield useful results.[40] Thus, in this survey, we examined the tradeoff between exposure to advertising and frequency of searches. Following increased exposure to the risk of litigation, firms offering search functions will have to increase the amount of advertising displayed on the search result pages. Our assumption here is that more prevalent or intrusive advertising on a search engine will reduce the number of searches individuals will undertake. Thus, in this survey we presented individuals with hypothetical search engines with varying levels of advertising and varying levels of maximum searches per day. We set the survey up in this way in order to measure the tradeoff between frequency of search and exposure to advertising—we do not assume that search engines will in fact impose a maximum number of searches in the future.

As with the cloud storage survey, the Internet search survey was administered to an online panel of 300 individuals who stated that they had used an Internet search service in the last week. After qualifying for the survey, respondents were presented with descriptions of seven attributes of Internet search engines they might wish to consider when conducting an Internet search. These attributes were (1) accuracy of the search results, (2) amount of advertising that must be viewed in order to see the search results,[41] (3), whether the search engine suggests search terms as the search query is entered, (4) the ability to filter results, (5) whether the search engine collects and shares search history, (6) the maximum number of searches per day, and (7) whether the search results are displayed in a mobile friendly way. A detailed description of the attributes and the levels of these attributes are presented in Appendix B.

Survey respondents were asked to make a series of choices from sets of hypothetical search engines, selecting the search engine they would be most likely to use. Each choice scenario shown to respondents presented three hypothetical search engines with a distinct combination of the seven attributes described above. Respondents were not given the option to decline to select a search engine under the assumption that Internet users will not abandon Internet search. An example of one choice scenario presented to respondents is shown in Table 4.

Table 4. **Example of a Choice Scenario in the Internet Search Conjoint Analysis**

Assuming that these three internet search engines are the only ones available to you, which internet search engine are you MOST likely to use?

For additional information about each feature, hover your mouse over or tap the bolded words.

Scenario 1 of 12 *(Select one)*

	Option 1	Option 2	Option 3
Accuracy	70%	90%	90%
Advertising	5 seconds	20 seconds	10 seconds
Autocomplete Capability	No	Yes	Yes
Categorization	No	Yes	Yes
Data Sharing	No	Yes	Yes
Maximum Searches per Day	25	5	1
Mobile Friendly	Yes	No	No
Your Choice	❑	❑	❑

As with the cloud storage survey, each respondent was presented with 12 different choice scenarios in total, giving us a total of 3,600 choices from among these hypothetical search engines.

We analyzed these choices with a conditional logit model, which allowed us to determine how each attribute influences the probability that an individual will use a given search engine. Again, the results were sensible—more accuracy, autocomplete capability, categorization of search results, mobile friendly results, and a higher number of maximum searches per day lead to higher probabilities of using the search engine, whereas advertising and sharing of search history reduce the probability of using the search engine. The results of estimating this conditional logit are presented in Table 5. These estimates are used to simulate the drop in demand for searches due to a hypothetical increase in advertising on search engines in the following section.

Table 5. **Conditional Logit Analysis of Internet Search Choices**

Attribute	Coefficient	Standard Error	Z-Score
Accuracy (%)	6.1578	0.2409	25.56
Advertising	-0.0334	0.0022	-14.99
Autocomplete Capability	0.2372	0.0427	5.56
Categorization	0.1161	0.041	2.83
Data Sharing	-0.2513	0.0393	-6.4
Maximum Searches per Day	0.0499	0.0024	20.55
Mobile Friendly	0.3672	0.0408	9

The market simulations to estimate the drop in search function demand is discussed in Section C below.

Market Simulations to Estimate Drop in Demand

Required price increase with a reduction in safe harbor protection

We begin with estimates of how much Internet intermediaries might be forced to raise prices if safe harbor protections are reduced. In these simulations, we assumed that any price increase would be solely used to cover the additional legal costs and potential liabilities that would emerge with a reduction in safe harbor protection.

These market simulations are a partial equilibrium analysis, only considering the increase in price and the resulting decrease in demand. We did not consider other steps that companies might take in response to decreased demand (such as cloud storage services offering less initial free storage space).

For consumer oriented cloud storage services, we used the MP3Tunes case as the basis for illustrating the magnitude of a potential price increase. The ultimate judgment against MP3Tunes was $41.5 million for infringements of music copyrights for offering music storage facilities. The infringement took place over approximately seven years, and MP3Tunes had approximately 125,000 users.[42] This judgment cost about $4.00 per customer per month.

For Internet search, we estimate the increase in revenue following greater exposure to advertisements. Price increases in this market simulation are measured as seconds of advertising. Each additional advertisement is expected to bring in approximately $0.002 cents in revenue.[43] Thus, if each ad takes about one second to view,[44] to raise an additional $1 per customer per month, this hypothetical search engine would need to add approximately five seconds of advertising per search. Although this would potentially raise significant revenue, about $400 million per month based on the number of searches in the United States, it needs to be kept in mind that the search services market is significantly larger than that of consumer cloud services. On a per-customer basis, the revenue generated is also lower than that awarded in the MP3Tunes litigation.

We used $4.00 per customer per month for consumer cloud services and five seconds of additional advertising for search services as our main approximations for the additional costs of a reduction in safe harbor protection. We also considered lower figures ($3.00 for cloud services and three seconds for search services) to represent scenarios where Internet intermediaries anticipate lower risks from the reduction in safe harbor protection.

Changing demand for cloud storage

From the conditional logit results for the cloud storage survey, we were able to undertake a market simulation to determine how demand for this Internet service would drop if the price was increased. Given the variety of cloud storage services available to consumers, this market simulation could grow quite complicated. Thus, we simplified the market to a single "average" cloud storage service.[45] In our market simulation, consumers choose between this average service and no service.

Thirty-two percent of respondents to our survey reported having a cloud storage service. Using the coefficients from the conditional logit model presented in Table 1, we calculated the probability that a consumer would select this average cloud storage service, adding a constant term to calibrate this predicted market share to the observed market share of 32 percent.

We then calculated how this market share would decline as the price of cloud storage increased. As explained in the previous section, we considered increases in price of $3.00 and $4.00. This gave us the drop in demand for cloud storage under various scenarios for price increases due to a reduction in safe harbor protection. The results of this market simulation are presented in Table 6.

Table 6. **Market Simulation for Cloud Storage Services**

Price	Market Share	% Change
$9.99 (baseline)	32.2%	--
$12.99 (+ $3.00)	28.1%	-10.7%
$13.99 (+ $4.00)	26.8%	-14.7%

In our calculations, we assumed that revenue was linear in demand and used these declines in demand as our figures for declines in revenue due to price increases. Note that in this market simulation demand for cloud storage service as estimated by the conditional logit model is relatively inelastic (approximately 0.37).

We discuss the impact of using an average drop of 14.7 percent on sector revenue and employment below. The impact of a 10.7 percent drop is shown in Appendix B.

Changing demand for Internet search

We also undertook a market simulation using the conditional logit results for the Internet search survey. In this case, we determined how demand for this Internet service would drop if the amount of advertising increased. Unlike cloud storage services, Internet search services are typically free, and it is unlikely that individuals would give up this service entirely. Thus, we conducted this simulation in a different way and examined the tradeoff that consumers would make between the maximum number of searches and seconds of advertising in our conjoint analysis.

By the properties of the conditional logit model, we can estimate the relative values of two attributes by examining the ratio of their coefficients. The ratio of the maximum searchers per day coefficient to the advertising coefficient is approximately –1.5. This demonstrates that, on average, consumers are willing to trade 1.5 searches to avoid one second of advertising. We then calculated the percentage drop in Internet searches as the seconds of advertising that must be viewed increases.

We considered the effect of an additional three seconds and additional five seconds of advertising. This gave us the drop in demand for Internet search under various scenarios for advertising increases due to a reduction in safe harbor protection. The results of this market simulation are presented in Table 7.

Table 7. **Market Simulation for Internet Search Services**

Advertising	% Change
Baseline	--
+ 3 seconds	-4.6%
+ 5 seconds	-7.6%

We discuss the impact of using an average drop of 7.6 percent on sector revenue and employment below. The impact of a 4.6 percent drop is shown in Appendix B.

Reducing Safe Harbors Will Hurt Search and Cloud Service Segments

The "Measuring the U.S. Internet Sector" study calculated the Internet industries' receipts in 2012 as totaling $352.1 billion using the North American Industry Classification System (NAICS), the standard used by the U.S. government.[46] Within the larger NAICS categories, the study selected those codes related to the Internet based on descriptions of their function, as well as the details contained in the "Product Line" Receipts published by the Census Bureau. From these numerous NAICS code subcategories, we selected the two categories previously discussed for further analysis, namely, Internet Publishing and Broadcasting, and Web Search Portals (NAICS code 51913) with the description "Publishing - Sale of advertising space - Internet" and Data Processing, Hosting, and Related Services (NAICS code 581210) with the description "Data storage services."

In 2012, the last year for which the "Measuring the U.S. Internet Sector" data are available, Internet advertising receipts reached $44.8 billion.[47] This compares well to the $36.6 billion of Internet advertising revenue estimated by the Interactive Advertising Bureau (IAB) for 2012. The IAB estimated that in 2015, Internet advertising revenue reached $59.6 billion.[48] "Measuring the U.S. Internet Sector" reports that consumer oriented data storage service receipts totaled $1.8 billion in 2012.[49] This compares to a 2013 estimate of $1.2 billion based on Dropbox's 17 percent share of storage services and its $200 million revenue.[50] This segment, although currently relatively small, is forecasted to grow rapidly with, for example, global consumer oriented storage services forecasted to grow by 40 percent per year between 2012 and 2018.[51]

The U.S. Internet Sector study estimates multipliers for entire NAICS codes. The multipliers are for gross output,[52] value added,[53] employee earnings, total employment, direct employment, and direct employee earnings. For the purposes of this report, which is trying to establish orders of magnitude, we assumed that the multipliers applicable to an entire NAICS category were also applicable to the subcategories within that NAICS category. Although the increase in litigation-related costs following any weakening of the current safe harbor protections would have a significant negative impact on the revenue and employment levels of these two categories, we assumed modest revenue impacts based on relatively small changes in costs modeled in the surveys.

The approach to measuring the impact of increased litigation exposure assumes that the Internet segments analyzed would retain their current business structure and deal with the additional liability expenses by passing the cost through to the user, either in the form of higher prices or increased advertising. Thus, for example, the search function would continue to search the entire Internet and would not limit itself to preapproved sites.

The Economic Impact on Internet Search

The results from the Internet survey showed a likely 7.6 percent reduction in Internet advertising receipts following the reduction in U.S. safe harbor protections. As shown in Table 8, such a reduction in receipts translates into a drop of about $8 billion in gross output annually, more than 51,000 in overall employment (of which 18,000 are direct employees), and $2.9 billion annually in overall employee earnings (of which direct employee earnings are $1.6 billion annually). In total, U.S. GDP (value added) would drop by $4.7 billion annually. These results do not pick up the impact of any diminution in international revenues that would likely follow as the result of the reduction in U.S. safe harbor protections, as other countries likely would feel emboldened to enact similar laws.

Table 8. **Assumed Reduction in Receipts: Publishing–Sale of Advertising Space–Internet**

Internet Publishing and Web Search Portals
NAICS 51913
2012
Publishing–Sale of Advertising Space–Internet

Estimated Reduction in Receipts *7.6%*

	Base	Impacted ($ million)	Difference
Final Demand			
Gross Output	$104,675	$96,720	$(7,955)
Employee Earnings	$38,208	$35,304	$(2,904)
Employment	673,992	622,769	(51,223)
Value-Added	$61,896	$57,192	$(4,704)
Direct Employment			
Final Demand Total Employment	673,992	622,769	
Direct Effect Multiplier	2.85	2.85	
Direct Employment	236,489	218,515	(17,973)
Direct Employee Earnings			
Total Earnings	$38,208	$35,304	
Direct Effect Multiplier	1.86	1.86	
Direct Earnings	$20,542	$18,981	$(1,561)

The Economic Impact on Cloud Storage

The results from the consumer oriented cloud data storage survey showed a likely 14.7 percent reduction in receipts following the reduction in U.S. Internet safe harbor protections.[54] As shown in Table 9, such a reduction in receipts would translate into a drop of over $500 million annually in gross output, about 2,300 in overall employment (of which around 670 would be direct employees), and $110 million annually in overall employee earnings (of which direct employee earnings would be $43 million annually). In total, U.S. GDP (value added) would drop by over $290 million annually. These economic impacts are smaller than that of search but would become more pronounced as the sector grows. It is expected to grow rapidly, with the global consumer oriented cloud storage market forecasted to grow by 40 percent between 2012 and 2018.[55]

Table 9. **Assumed Reduction in Receipts: Data Storage Services**

Data Processing, Hosting and Related Services
NAICS 518210
2012
Data Storage Services

Estimated Reduction in Receipts *14.7%*

	Base	Impacted ($ million)	Difference
Final Demand			
Gross Output	$3,452	$2,945	$(507)
Employee Earnings	$745	$636	$(110)
Employment	15,712	13,402	(2,310)
Value-Added	$1,966	$1,677	$(289)
Direct Employment			
Final Demand Total Employment	15,712	13,402	
Direct Effect Multiplier	3.46	3.46	
Direct Employment	4,541	3,873	(668)
Direct Employee Earnings			
Total Earnings	$745	$636	
Direct Effect Multiplier	2.53	2.53	
Direct Earnings	$295	$251	$(43)

Reducing Safe Harbors Will Hurt the Entire Internet Sector

Direct Effects on the U.S. Internet Sector

The consumer surveys focused on two Internet intermediary services, consumer oriented cloud storage and Internet search. These account for about 18 percent of all intermediary Internet services revenue. There are many more Internet intermediaries, and the reduction in safe harbor protections would affect most of these companies.

To estimate the potential impact on the overall U.S. Internet sector, we calculated the revenue-weighted average decrease in receipts from Internet search and cloud services. Specifically, the relevant NAICS codes for search report receipts of $73.2 billion, whereas the NAICS codes for all cloud storage generate $47.5 billion. A weighted average of the survey results (i.e., a demand reduction of 7.6 percent and 14.7 percent for search and all cloud services, respectively) results in a reduction in revenues of approximately 10 percent.

Using this 10 percent revenue drop as an indicator of the percentage decrease for the *entire* U.S. Internet sector indicates that a reduction in safe harbor protection would cost the U.S. economy $75 billion annually, lower employee earnings by some $23 billion annually, and eliminate over 425,000 jobs. The U.S. gross domestic product would decrease by $44 billion annually. The overall impact on the U.S. economy is summarized in Table 10.[56]

Table 10. **All NAICS Categories Summary, 2012**

Total Receipts ($ million)	*$352,127*
Assumed Reduction in Receipts	*10.0%*

	Base	Impacted ($ million)	Difference
Final Demand			
Gross Output	$753,088	$677,780	$(75,309)
Employee Earnings	$225,861	$203,275	$(22,586)
Employment	4,285,827	3,857,245	(428,583)
Value-Added	$438,657	$394,792	$(43,866)
Direct Employment			
Final Demand Total Employment	$4,285,827	$3,857,245	
Direct Effect Multiplier	3.05	3.05	
Direct Employment	$1,404,700	$1,264,230	(140,470)
Direct Employee Earnings			
Total Earnings	$225,861	$203,275	
Direct Effect Multiplier	2.02	2.02	
Direct Earnings	$111,864	$100,677	$(11,186)

Secondary Effects on the U.S. Internet Sector

In addition to the more easily measurable negative direct effects on the U.S. economy, a reduction in safe harbor protections will also have negative secondary effects that are not easily quantifiable. In particular, there is evidence that it will reduce the formation of new Internet intermediary startups, as well as reduce investment in the Internet more generally.

Emerging technological businesses are considered the drivers of future economic growth in the United States. Investments made by venture capitalists are an important factor in the early stage development of Internet intermediaries. Because many of the Internet intermediary business models consist of distributed digital content and the amount of this content has grown hugely, their ability to operate within safe harbors has grown more important. The regulatory and legal environment is particularly important to U.S. startup investors, as shown in a 2014 survey.[57] According to the survey, 93 percent of respondents found legal ambiguity (defined as concern about regulatory environment, uncertain and potentially large damages, and IP infringement) as having a negative impact on startup investment. Of the respondents, 89 percent stated it would negatively affect "investing in digital content intermediaries that offer user generated music and video" as these intermediaries "are particularly exposed to potential new legislation, and the current legal environment…."

A 2016 survey of U.S. investors found a similar result, with 94 percent of investors stating that an uncertain legal environment had negative consequences for investment and with 76 percent of investors concerned about exposure to very large damages.[58]

Thus, although our consumer survey estimated the potential direct impact on the usage of consumer storage and Internet search from an increase in costs, these investor surveys indicate that there are also significant potential secondary effects that would harm the U.S. economy.

Conclusion

The U.S. Internet sector is one of our nation's most successful economic performers, both here and internationally. As we have detailed, the reduction in Internet safe harbor protections would likely have severe negative economic consequences on U.S. employment as well as on the U.S. GDP.

Appendix A: Cloud Search Survey

Attributes and Levels in Cloud Storage Conjoint Analysis

Attribute Descriptions

Automatic Backup – whether the cloud data storage service automatically backs up one or multiple devices (e.g., smartphone, laptop) to the cloud. Devices can still be backed up manually if automatic backup is not available.

Encryption – whether the stored files are encrypted. Encryption provides an additional level of security for stored files.

File Sharing – available options for allowing others to view, download, and/or edit files.

File Size Restrictions – maximum size of an individual file that can be uploaded to the cloud (the average high definition movie is about 3-5 GB).

Price – monthly subscription price, in dollars.

Storage – amount of monthly storage included in plan (1 GB of space will hold approximately 240 songs or 300 photos, whereas 1000 GB of space will hold approximately 300 high definition movies).

Attribute Levels

Automatic Backup	Encryption	File Sharing	File Size Restrictions	Price	Storage
No	No	No file sharing	250 MB	$1.99	5 GB
One device	Yes	View or download only	1 GB	$5.99	10 GB
Multiple devices		View, download, and real-time editing	2 GB	$9.99	50 GB
			5 GB	$15.99	100 GB
			10 GB	$19.99	500 GB
			Unlimited	$24.99	1000 GB

Attributes and Levels in Internet Search Conjoint Analysis

Attribute Descriptions

Accuracy – The percentage of searches that return a relevant result on the first page.

Advertising – Length of video advertising, in number of seconds, that must be watched to access search results.

Autocomplete Capability – The ability of the search engine to suggest search terms while you enter your search query.

Categorization – The ability to filter search results by images, videos, maps, and news stories.

Data Sharing – The extent to which the search engine collects and shares your search history.

Maximum Searches per Day – The maximum number of searches the search engine allows per day. The average person makes about 5 searches per day.

Mobile Friendly – Whether the search results are easy to read on mobile devices.

Attribute Levels

Accuracy	Advertising	Autocomplete Capability	Categorization	Data Sharing	Max Daily Searches	Mobile Friendly
70%	0 seconds	Yes	Yes	Yes	1	Yes
75%	5 seconds	No	No	No	5	No
80%	10 seconds				10	
85%	15 seconds				15	
90%	20 seconds				20	
95%	30 seconds				25	

Appendix B: Internet Search Survey

In this appendix, we briefly discuss the economic impacts of lesser litigation-related expense assumptions, which still show very significant negative economic consequences of reducing Internet safe harbor protections.

The results from the Internet survey showed a likely 7.6 percent reduction in Internet advertising receipts following the reduction in the United States of Internet safe harbor protections. If, instead, there was a 4.6 percent reduction in receipts based on three additional ads per search,[59] as shown in Table 11, such a reduction in receipts translates into a drop of about $4.8 billion in gross output annually, 31,000 in overall employment (of which close to 11,000 are direct employees), and $1.8 billion annually in overall employee earnings (of which direct employee earnings are about $950 million annually). In total, U.S. GDP (value added) would drop by $2.8 billion annually. These results do not pick up the impact of any diminution in international revenues that would likely follow as the result of the reduction in U.S. safe harbor protections as other countries likely would feel emboldened to enact similar laws.

Table 11. **Alternative Reduction in Receipts: Publishing–Sale of Advertising Space–Internet**

Internet Publishing and Web Search Portals
NAICS 51913
2012
Publishing–Sale of Advertising Space–Internet

Assumed Reduction in Receipts *4.6%*

	Base	Impacted ($ million)	Difference
Final Demand			
Gross Output	$104,675	$99,860	$(4,815)
Employee Earnings	$38,208	$36,451	$(1,758)
Employment	673,992	642,989	(31,004)
Value-Added	$61,896	$59,049	$(2,847)
Direct Employment			
Final Demand Total Employment	673,992	642,989	
Direct Effect Multiplier	2.85	2.85	
Direct Employment	236,489	225,610	(10,878)
Direct Employee Earnings			
Total Earnings	$38,208	$36,451	
Direct Effect Multiplier	1.86	1.86	
Direct Earnings	$20,542	$19,597	$(945)

The results from the consumer oriented cloud data storage survey showed a likely 14.7 percent reduction in receipts following the reduction in U.S. Internet safe harbor protections. If, instead there was a 10.7 percent reduction in receipts based on a $3 increase in storage costs per month, as shown in Table 12, such a reduction in receipts would translate into a drop of about $370 million annually in gross output, about 1,700 in overall employment (of which about 490 would be direct employees), and $80 million annually in overall employee earnings (of which direct employee earnings would be about $30 million annually). In total, U.S. GDP (value added) would drop by over $200 million annually.

Table 12. **Alternative Reduction in Receipts: Publishing–Sale of Advertising Space–Internet**

Data Processing, Hosting and Related Services
NAICS 518210
2012
Data Storage Services

Assumed Reduction in Receipts *10.7%*

	Base	Impacted ($ million)	Difference
Final Demand			
Gross Output	$3,452	$3,083	$(369)
Employee Earnings	$745	$666	$(80)
Employment	15,712	14,031	(1,681)
Value-Added	$1,966	$1,755	$(210)
Direct Employment			
Final Demand Total Employment	15,712	14,031	
Direct Effect Multiplier	3.46	3.46	
Direct Employment	4,541	4,055	(486)
Direct Employee Earnings			
Total Earnings	$745	$666	
Direct Effect Multiplier	2.53	2.53	
Direct Earnings	$295	$263	$(32)

About the Author

Dr. Dippon is the Chair of NERA's Energy, Environment, Communications, and Infrastructure Practice and a Managing Director in NERA's Washington, DC office. He specializes in the economics and business of the communications and high-tech industries, advising his clients in complex litigation disputes, antitrust matters, and regulatory and policy issues. Dr. Dippon has extensive testimonial experience, including depositions and expert testimonies before state and federal courts, the Federal Communications Commission, the International Trade Commission, numerous state commissions, and international courts and regulatory authorities.

With over 20 years of experience, Dr. Dippon is an internationally renowned expert in communications, with deep expertise in Internet, wireline, wireless, cable, and equipment markets. Dr. Dippon has consulted to clients in countries around the world, including the United States, Australia, Brazil, Canada, China, the Dominican Republic, Greece, Hong Kong, Hungary, Indonesia, Ireland, Israel, Japan, Korea, Malaysia, New Zealand, Palestine, Qatar, Singapore, Spain, Thailand, Turkey, United Arab Emirates, and the United Kingdom.

Dr. Dippon has authored and edited several books as well as book chapters in anthologies and has written numerous articles on telecommunications competition and strategies. He also frequently lectures in these areas at industry conferences, continuing education programs for lawyers, and at universities. National and international newspapers and magazines, including the *Financial Times*, *Businessweek*, *Forbes*, the *Chicago Tribune*, and *The Sydney Morning Herald* have cited his work.

Dr. Dippon serves on the Board of Directors of the International Telecommunications Society (ITS) and on the Editorial Board of Telecommunications Policy. He is a member of the Economic Club of Washington, DC, the American Economic Association (AEA), the American Bar Association (ABA), and the Federal Communications Bar Association (FCBA).

Dr. Dippon holds a PhD and an MA in economics and an undergraduate degree in business administration. He is bilingual in English and German and proficient in French and Thai. Prior to joining NERA, Dr. Dippon was an analyst at BMW in Bangkok.

Notes

[1] OECD, "The Economic and Social Role of Internet Intermediaries," April 2010, p. 9.

[2] www.internetlivestats.com/google-search-statistics.

[3] 47 U.S.C. § 230(b)(1).

[4] 47 U.S.C. § 230(c)(1).

[5] Digital Law Online, Chapter 3: Copyright of Digital Information III.B. Congress Codifies the Decisions, 2002, http://digital-law-online.info/lpdi1.0/treatise33.html.

[6] 17 U.S.C. § 512(a); § 512(b)(1); §512(c)(1); § 512(d).

[7] 17 U.S.C. § 512(i)(1)(A).

[8] European Commission, Commission Communication to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, Jan. 11, 2012, p. 13.

[9] Internet Association, "Position Paper on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy," Dec. 2015, p. 8.

[10] Stephen E. Siwek, *Measuring the U.S. Internet Sector* (Internet Association, December 2015), pp. 5–8, 11, http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf (hereafter Measuring the U.S. Internet Sector).

[11] *Stuart Force, et al. v. Facebook Inc.*, U.S. District Court for the Southern District of New York, case number 1:16-cv05158, 2016, ¶¶ 4, 337; *Tamara Fields, et al., v. Twitter, Inc.*, U.S. District Court for the Northern District of California, case number 16-ev-00213-WHO, 2016.

[12] Memorandum of Opinion, *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, United States District Court for the Eastern District of Virginia, Civil No. 1:14-cv-1611, Aug. 8, 2016, p. 1 (*BMG v. Cox, Opinion*).

[13] The Court had instructed the jury that the "amount awarded must be between $750 and $30,000 for each copyrighted work that you found to be infringed." (*BMG v. Cox*, Opinion, pp. 1, 37).

[14] *EMI Christian Music Grp., Inc. et al. v. MP3tunes, LLC et al.*, U.S. District Court of Appeals for the Second Circuit, Docket Nos. 14-4369-cv(L), 14-4509-cv(XAP), Oct. 25, 2016, p. 3 (hereafter MP3tunes Decision).

[15] MP3tunes Decision, p. 5.

[16] MP3tunes Decision, pp. 9–10.

[17] MP3tunes Decision, p. 27.

[18] MP3tunes Decision, p. 49.

[19] European Commission, Factsheet on the "Right to be Forgotten" ruling (C-131/12), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf. (Emphasis in original.)

[20] European Commission, Factsheet on the "Right to be Forgotten" ruling (C-131/12).

[21] Farhad Manjoo, "'Right to Be Forgotten' Online Could Spread," *The New York Times*, Aug. 5, 2015.

[22] Information Commissioner's Office, https://ico.org.uk/about-the-ico/who-we-are.

[23] Sophie Curtis, "EU 'right to be forgotten': one year on," *The Telegraph*, May 13, 2015.

[24] Allison Grande, "NY's 'Right To Be Forgotten' Bill Needs Narrower Focus," *Law360*, Mar. 28, 2017.

[25] Jennifer Stanley and Liwen A. Mah, "EU Court Brings New Copyright Liability for Linked Material," Law360, Oct. 7, 2016.

[26] *GS Media BV v. Sanoma Media Netherlands BV, et al.*, Judgment of the Court (Second Chamber) case C-160/15, Sept. 8, 2016, ¶ 51.

[27] Jennifer Stanley and Liwen A. Mah, "EU Court Brings New Copyright Liability For Linked Material," *Law360*, Oct. 7, 2016.

[28] Binyamin Appelbaum, "Investors Put Money on Lawsuits to Get Payouts," *The New York Times*, November 14, 2010, http://www.nytimes.com/2010/11/15/business/15lawsuit.html; see also U.S. Chamber Institute for Legal Reform, *Selling Lawsuits, Buying Trouble: Third Party Litigation Funding In The United States* (hereafter U.S. Chamber Institute for Legal Reform, 2009), p. 1.

[29] Measuring the U.S. Internet Sector, p. 39.

[30] Income generated from production consists of payments to labor (compensation of employees), payments to government (taxes on production and imports), and returns on investment (gross operating surplus). The sum of these categories equals value added.

[31] Measuring the U.S. Internet Sector, pp. 5, 7–8.

[32] Measuring the U.S. Internet Sector, pp. 7–8.

[33] OECD, "Measuring the Internet Economy: A Contribution to the Research Agenda," OECD Digital Economy Papers, No. 226, 2013, p. 29.

[34] Erik Brynjolfsson and Andrew McAffee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W. W. Norton & Company, 2014), cited in Nadim Ahmad and Paul Schreyer, "Measuring GDP in a Digitalised Economy," OECD Statistics Working Papers, June 17, 2016, p. 11, DOI: 10.1787/5jlwqd81d09r-en (hereafter Measuring GDP in a Digitalised Economy).

[35] Measuring GDP in a Digitalised Economy, p. 5.

[36] eMarketer, "Facebook Mobile Ad Revenues to Near $30 Billion Next Year," Oct. 31, 2016, https://www.emarketer.com/Article/Facebook-Mobile-Ad-Revenues-Near-30-Billion-Next-Year/1014658.

[37] eMarketer, "Mobile Moves to Majority Share of Google's Worldwide Ad Revenues," Oct. 24, 2016.

[38] Brad Reed, "iCloud revealed as America's most-used cloud storage service," *BGR.com*, Mar. 21, 2013.

[39] Conditional logit models are appropriate when the choice among alternatives is modeled as a function of the characteristics of the alternatives instead of the characteristics of the respondents making the choice.

[40] It is certainly possible that a search-engine service with a subscription fee could emerge if safe harbor protections were reduced with the subscription price of the search engine covering the same legal costs that search engines would cover with increased advertising in our experiment. However, designing an experiment around search engines with subscription fees could lead to unexpected results. For instance, there is a risk of an "endowment effect" with survey respondents objecting to the concept of paying for something they currently receive for free. This could lead to protest answers (e.g., respondents stating they would not use any Internet search engines) or refusing to complete the survey rather than making tradeoffs between price and search behavior.

Notes

[41] In the survey, the amount of advertising is presented as the "length of video advertising, in number of seconds, that must be watched to access search results." We present advertising to our survey subjects in this way to clarify the tradeoff between advertising intensity and search behavior. We do not assume that search engines will introduce video advertising in response to a weakening of safe harbor provisions.

[42] MP3tunes Decision, p. 10; Timothy B. Lee, "Music labels force pioneering MP3tunes into bankruptcy," *arstechnica.com*, May 14, 2012, https://arstechnica.com/tech-policy/2012/05/music-labels-force-pioneering-mp3tunes-into-bankruptcy; Michael Robertson, "Court Ruling Denies EMI Access to Millions of Personal MP3 Files," *michaelrobertson.com*, http://www.michaelrobertson.com/archive.php?minute_id=259.

[43] This estimate is substantially based on public data for Google. Google completes about 115 billion searches per month conducted by about 1.17 billion unique users, or about 100 searches per user per month. The average number of ads displayed equals about eight per search. The Google segment of Alphabet had approximately $23 billion in operating income in 2015. This results in revenue per ad of $0.002. With five additional sponsored links per search, each user would generate about $0.011 in additional income per search. This equates to about $1.00 per user per month. Thus, with about 40 million total searches conducted in the United States, each sponsored link is expected to generate approximately $400 million in revenue per month. (See D. Sullivan, "Google Still World's Most Popular Search Engine by Far, But Share of Unique Searchers Dips Slightly," *searchengineland.com*, Feb. 11, 2013; Alphabet Inc., Form 10-K, December 2015, p. 95; L. Kim, "How Many Ads Does Google Serve in a Day?" *business2community.com*, Nov. 2, 2012; comScore, "comScore Releases February 2016 U.S. Desktop Search Engine Rankings," Mar. 16, 2016; G. Sterling, "Report: Nearly 60 percent of searches now from mobile devices," *searchengineland.com*, Aug. 3, 2016.)

[44] This calculation assumes all ads on the search engine are text-based ads; the average text ad is 125 characters, and the average reader can read 1,000 characters per minute. See https://support.google.com/adwords/answer/1704389?hl=en and https://en.wikipedia.org/wiki/Words_per_minute.

[45] This "average" service offers 1,000 GB of storage, encryption, automatic backup for multiple devices, the ability to allow others to view and download files, and a maximum file upload size of 500 GB, and costs $9.99 per month.

[46] Measuring the U.S. Internet Sector, p. 39.

[47] Measuring the U.S. Internet Sector, p. 57.

[48] IAB, "IAB internet advertising revenue report," Nov. 2016, p. 10.

[49] Measuring the U.S. Internet Sector, p. 53.

[50] Brad Reed, "iCloud revealed as America's most-used cloud storage service," *BGR.com*, Mar. 21, 2013; see also "The Cloud Storage Battle: Box vs. Dropbox," *computersciencedegreehub.com*, http://www.computersciencedegreehub.com/cloud-storage-battle.

[51] "The Cloud Storage Battle: Box vs. Dropbox," *computersciencedegreehub.com*.

[52] Gross output equals total market value of industry output (sales). It equals intermediate inputs plus value added.

[53] Value added equals total value of income generated from production. This income consists of payments to labor (compensation of employees), payments to government (taxes on production and imports), and returns on investment (gross operating surplus). The sum of these parts equals gross domestic product (GDP).

[54] Since the impact is measured relative to receipts any diminution in the availability of free storage is not captured.

[55] "The Cloud Storage Battle: Box vs. Dropbox," *computersciencedegreehub.com*.

[56] Measuring the U.S. Internet Sector, pp. 26–31.

[57] Matthew C. LeMerle, Tallulah J. LeMerle, and Evan Engstrom, "The Impact of Internet Regulation on Early Stage Investment," *Fifth Era*, November 2014, p. 40.

[58] Matthew C. LeMerle, Alison Davis, and Felix O. LeMerle, "The Impact of Internet Regulation on Investment," *Fifth Era*, January 2016, p. 91.

[59] This would generate approximately an estimated $0.60 per search function user per month and, based on the number of searches in the United States total, to about $260 million in revenue per month.

NERA
ECONOMIC CONSULTING

About NERA

NERA Economic Consulting (**www.nera.com**) is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal challenges. For over half a century, NERA's economists have been creating strategies, studies, reports, expert testimony, and policy recommendations for government authorities and the world's leading law firms and corporations. We bring academic rigor, objectivity, and real world industry experience to bear on issues arising from competition, regulation, public policy, strategy, finance, and litigation.

NERA's clients value our ability to apply and communicate state-of-the-art approaches clearly and convincingly, our commitment to deliver unbiased findings, and our reputation for quality and independence. Our clients rely on the integrity and skills of our unparalleled team of economists and other experts backed by the resources and reliability of one of the world's largest economic consultancies. With its main office in New York City, NERA serves clients from more than 25 offices across North America, Europe, and Asia Pacific.

Contact

For further information and questions, please contact the author:

Dr. Christian Dippon
Managing Director
Chair of NERA's Global Energy, Environment, Communications and Infrastructure Practice
+1 202 466 9270
christian.dippon@nera.com

NERA
ECONOMIC CONSULTING

Visit **www.nera.com** to learn more about our practice areas and global offices.

JOHN P. COALE *(pro hac vice)*
2901 Fessenden Street NW
Washington, DC 20008
Telephone: (202) 255-2096
Email: johnpcoale@aol.com

JOHN Q. KELLY *(pro hac vice)*
MICHAEL J. JONES *(pro hac vice)*
RYAN TOUGIAS *(pro hac vice)*
IVEY, BARNUM & O'MARA, LLC
170 Mason Street
Greenwich, CT 06830
Telephone: (203) 661-6000
Email: jqkelly@ibolaw.com

FRANK C. DUDENHEFER , JR. *(pro hac vice)*
THE DUDENHEFER LAW FIRM L.L.C.
2721 Saint Charles Avenue, Suite 2A
New Orleans, LA 70130
Telephone: (504) 616-5226
Email: fcdlaw@aol.com
Attorneys for Plaintiffs

ANDREI POPOVICI (234820)
MARIE FIALA (79676)
LAW OFFICE OF ANDREI D. POPOVICI, P.C.
2121 North California Blvd. #290
Walnut Creek, CA 94596
Telephone: (650) 530-9989
Facsimile: (650) 530-9990
Email: andrei@apatent.com
Email: marie@apatent.com

RICHARD POLK LAWSON *(pro hac vice)*
GARDNER BREWER MARTINEZ MONFORT
400 North Ashley Drive
Suite 1100
Tampa, FL 33602
Telephone: (813) 221-9600
Facsimile: (813) 221-9611
Email: rlawson@gbmmlaw.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

DONALD J. TRUMP, the Forty-Fifth President of the United States, LINDA CUADROS, AMERICAN CONSERVATIVE UNION, RAFAEL BARBOSA, DOMINICK LATELLA, WAYNE ALAN ROOT, NAOMI WOLF, INDIVIDUALLY, AND ON BEHALF OF THOSE SIMILARLY SITUATED
Plaintiffs,
v.
TWITTER INC. and JACK DORSEY,
Defendants.

Case No: 3:21-cv-08378-JD

REQUEST FOR JUDICIAL NOTICE IN SUPPORT OF PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS

Hearing Date: February 24, 2022
Time: 10:00 a.m.
Place: Courtroom 11, 19th Floor
Judge: Hon. James Donato

Pursuant to Federal Rule of Evidence 201, Plaintiffs ask the Court to take judicial notice of the following documents in support of their Opposition to Motion to Dismiss:

1. Exhibit A, excerpts from Defendant Dorsey's responses to questions submitted for the Senate Judiciary Committee Hearing conducted on November 17, 2020 ("Breaking the News: Censorship, Suppression, and the 2020 Election"); full record of responses available at https://www.judiciary.senate.gov/imo/media/doc/Dorsey%20Response%20QFRs.pdf.

2. Exhibit B, Opening Statement as Prepared for Delivery of Committee Chairman Frank Pallone, Jr. for the House Committee on Energy and Commerce Hearing conducted on March 22, 2021 ("Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Opening%20Statement_Pallone_CAT-CPC_2021.3.25_0.pdf.

3. Exhibit C, Opening Statement as Prepared for Delivery of Subcommittee Chairman Mike Doyle for the House Committee on Energy and Commerce Hearing conducted on March 22, 2021 ("Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Opening%20Statement_Doyle_CAT-CPC_2021.3.25.pdf.

4. Exhibit D, Opening Statement as Prepared for Delivery of Subcommittee Chairman Janice D. Schakowsky for the House Committee on Energy and Commerce Hearing conducted on March 22, 2021 ("Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Opening%20Statement_Schakowsky_CAT-CPC_2021.3.25_0.pdf.

5. Exhibit E, Memorandum from Chairman Pallone prepared by Committee on Energy and Commerce Staff for the House Committee on Energy and Commerce Hearing ("Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation") conducted on March 22, 2021, available at

https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-20210325-SD002.pdf.

6. Exhibit F, Twitter, Inc. Form 10-K dated 2/17/2021, filed for the year ended 12/31/2020, available at https://www.sec.gov/Archives/edgar/data/0001418091/000141809121000031/twtr-20201231.htm.

Under Fed. R. Evid. 201, a court "may judicially notice a fact that is not subject to reasonable dispute because it…can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." *See Santa Monica Food Not Bombs v. City of Santa Monica*, 450 F.3d 1022, 1026 n.2 (9th Cir. 2006). Facts contained in public records are considered appropriate subjects of judicial notice, including the records and reports of administrative bodies. *Id. See also* United States v. *Ritchie,* 342 F.3d 903, 909 (9th Cir. 2003). In particular, judicial notice is appropriate under Fed. R. Evid. 201(b)(2) for information obtained from official governmental websites. *Paralyzed Veterans of Am. V. McPherson,* 2008 WL 4183981, at *5 (N.D. Cal. Sept. 8, 2008) (court took judicial notice of information from official government websites, citing multiple decisions from federal circuits and district courts).

A court may consider judicially noticeable materials without converting a motion to dismiss into a motion for summary judgment. *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003); *Mir v. Little Co. of Mary Hosp.*, 844 F.2d 646, 649 (9th Cir. 1988). Furthermore, under the "incorporation by reference" doctrine, a court may "take into account documents 'whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the [plaintiff's] pleading.'" *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

The November 2020 and March 2021 Congressional Hearings are referenced in Plaintiffs' First Amended Complaint at FAC ¶¶ 57-58 ("Breaking the News: Censorship, Suppression, and the 2020 Election": Hearing before S. Comm. on the Judiciary, 116th Cong. (2020); "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation": Hearing before H. Comm. on Energy and Com., 117th Cong. (2021)). The Court may take

judicial notice of these governmental records on a motion to dismiss. *Judan v. Wells Fargo Bank, National Association*, 2017 WL 3115172, at *1 (N.D. Cal. July 21, 2017), citing *Mack v. S. Bay Beer Distrib., Inc.,* 798 F.2d 1279, 1282 (9th Cir. 1986), *abrograted on other grounds by Astoria Fed. Sav. Loan Ass'n v. Solimino*, 501 U.S. 104 (1991).

Regarding Exhibit F, the Court may take judicial notice of the content of the Securities and Exchange Commission Form 10-K, and the fact that it was filed with the agency. *Gerritsen v. Warner Bros Entertainment Inc.*, 112 F. Supp.3d 1011, 1031-1032 (C.D. Cal. Jan. 30, 2015). ("Defendants […] contend that "Ms. Gerritsen cannot amend her complaint by attaching [corporate disclosure documents] to her brief in opposition to defendants' Motion to Dismiss." Courts can consider securities offerings and corporate disclosure documents that are publicly available. *See Metzler Inv. GMBH v. Corinthian Colleges, Inc.*, 540 F.3d 1049, 1064 n. 7 (9th Cir.2008). *See also Lovelace v. Software Spectrum Inc.*, 78 F.3d 1015, 1018 (5th Cir.1996) ("When deciding a motion to dismiss ..., a court may consider the contents of relevant public disclosure documents which (1) are required to be filed with the SEC, and (2) are actually filed with the SEC. Such documents should be considered only for the purpose of determining what statements the document contain, not to prove the truth of the documents' contents," citing *Hennessy v. Penril Datacomm Networks, Inc.*, 69 F.3d 1344, 1354–55 (7th Cir.1995)).

Plaintiffs respectfully ask that the Court take judicial notice of the existence and contents of the documents submitted as Exhibits A-F.

Dated: January 10, 2022

Respectfully submitted,

ANDREI POPOVICI (234820)
MARIE FIALA (79676)
LAW OFFICE OF ANDREI D. POPOVICI, P.C.

By: */s/ Andrei D. Popovici*
Andrei D. Popovici

JOHN P. COALE *(pro hac vice)*
2901 Fessenden Street NW
Washington, DC 20008
Telephone: (202) 255-2096
Email: johnpcoale@aol.com

JOHN Q. KELLY *(pro hac vice)*
MICHAEL J. JONES *(pro hac vice)*
RYAN TOUGIAS *(pro hac vice)*
IVEY, BARNUM & O'MARA, LLC
170 Mason Street
Greenwich, CT 06830
Telephone: (203) 661-6000
Email: jqkelly@ibolaw.com
Email: mjones@ibolaw.com

FRANK C. DUDENHEFER, JR. *(pro hac vice)*
THE DUDENHEFER LAW FIRM L.L.C.
2721 Saint Charles Avenue, Suite 2A
New Orleans, LA 70130
Telephone: (504) 616-5226
Email: fcdlaw@aol.com

RICHARD POLK LAWSON *(pro hac vice)*
GARDNER BREWER MARTINEZ MONFORT
400 North Ashley Drive
Suite 1100
Tampa, FL 33602
Telephone: (813) 221-9600
Facsimile: (813) 221-9611
Email: rlawson@gbmmlaw.com

Attorneys for Plaintiffs

EXHIBIT A

Questions from Senator Tillis

11. Do you coordinate with any other company or outside group when you make decisions about content moderation?

Twitter does not coordinate with other entities when making content moderation decisions. However, we have partnerships with government agencies, nonprofits, and industry peers to facilitate information sharing to inform our policy and enforcement decisions.

For example, the National Center for Missing & Exploited Children, whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization, is an important partner for Twitter and our industry peers. When we are made aware of content depicting or promoting child sexual exploitation, including links to images or content or third party sites where this content can be accessed, the material is removed without further notice and reported to NCMEC. While our general practice is to notify Twitter users when their content is reported to third-parties or law enforcement, we do not notify users when the reported content includes child sexual exploitation material. Furthermore, we participate in NCMEC's hash sharing database for industry and non-governmental organizations which consists of image and video hashes of known child sexual abuse material.

We also partner with nonprofits dedicated to child protection across the globe. In addition to our important relationship with NCMEC, Twitter is an active member of the Technology Coalition. This industry-led non-profit organization strives to eradicate child sexual exploitation by mentoring emerging or established companies, sharing trends and best-practices across industry, and facilitating technological solutions across the ecosystem. The Technology Coalition serves as an effective model because it gives companies the flexibility to create, test, and iterate across our diverse products and models

12. Does Twitter receive any information from any other company or entity other than Twitter about posts and content moderation decisions?

Twitter has numerous partnerships that we rely on to better inform policy and decision making. In addition to the partnerships described above, Twitter is part of the Global Internet Forum to Counter Terrorism, which brings together industry, government, civil society, and academia to share information and collaborate to counter terrorist or extremist content online. Through the

GIFCT, we have assembled a shared industry database of “hashes" or digital “fingerprints” for violent terrorist propaganda that spans more than 100,000 hashes. The database allows a company that discovers terrorist content on one of its sites to create a digital fingerprint and share it with the other companies in the forum, who can then use those hashes to identify such content on their services or platforms, review against their respective policies and individual rules, and remove matching content as appropriate or block extremist content before it is posted.

We also began to work with a small group of companies to test a new collaborative system to share URLs. Because Twitter does not allow files other than photos or short videos to be uploaded, one of the behaviors we saw from those seeking to promote terrorism was to post links to other services where people could access files, longer videos, PDFs, and other materials. Our pilot system allows us to alert other companies when we removed an account or Tweet that linked to material that promoted terrorism hosted on their service. This information sharing ensures the hosting companies can monitor and track similar behavior, taking enforcement action pursuant with their individual policies. This is not a high-tech approach, but it is simple and effective, recognizing the resource constraints of smaller companies

In order to safeguard the conversation regarding the 2020 U.S. election, we also have partnerships with leaders in civic tech, industry, and governments organizations, such as the National Association of Secretaries of State, National Association of State Election Directors, Department of Homeland Security, Federal Bureau of Investigation, Department of Justice, Office of the Director of National Intelligence, and elections officials across the country. We have also developed partnerships with news organizations, civil society, and others, which have been instrumental in informing policies and helping to identify potential threats regarding the integrity of the election conversation occurring on Twitter.

Questions from Senator Blackburn

1. During the November 3, 2020 election (before and after this date), did Twitter maintain any informal or formal lists of U.S. public officials who were specifically targeted for special monitoring of their Twitter posts?

During the election period, we used a combination of human and automated mechanisms to enforce our policies. For example, we reviewed Tweets reported as potential violations by the public, civil society partners, or government agencies. We also used automated systems to detect suspicious behaviors or identify potential violations of our rules. Twitter's enforcement teams prioritized the review of Tweets from the accounts of each of the presidential candidates and their campaigns and reviewed each to ensure compliance with our terms of service, beginning two weeks prior to election day.

Questions from Senator Cruz

4. The day before you testified before the Committee, you and I spoke on the telephone and you told me that Twitter was committed to transparency with regard to its content moderation policies and enforcement. Accordingly, the following questions relate to Twitter's enforcement of its content moderation policies. For this question and its subparts, please construe "content moderation policies" broadly, including decisions regarding the position or order in which content is displayed, the position or order in which users or content appear in searches, whether users or content are promoted or demoted, and all other modifications of content, such as flagging, qualifying, labelling, and denoting.

[…]

d. In drafting Twitter's election information content moderation policies and enforcing those same policies with regard to the 2020 elections, did Twitter collaborate with, confer with, or defer to any outside individuals or organizations? If so, please list the individuals and organizations and state the nature of their relationship with Twitter.

As part of our civic integrity efforts, we have developed partnerships that allowed us to share information, gather input from experts, and better gain context on how misinformation was being spread and impacting the public conversation. These partnerships included leaders in civic tech, our peers, federal, state, and local governments organizations (e.g., National Association of Secretaries of State, National Association of State Election Directors, Department of Homeland Security, Federal Bureau of Investigation, Department of Justice, Office of the Director of National Intelligence, and elections officials across the country), news organizations, and civil society, among others.

Questions from Senator Hawley

1. Does Twitter have a policy prohibiting its employees from coordinating content moderation decisions with outside companies such as Facebook or Google, where such moderation is not strictly required by law?

Twitter does not coordinate its content moderation decisions with outside entities. However, Twitter has numerous partnerships that we rely on to better inform decision making and facilitate information sharing. For example, we share information in three critical areas: combatting child sexual exploitation, prohibiting terrorism and violent extremism, and safeguarding the conversation about the U.S. election.

The National Center for Missing & Exploited Children is a nonprofit whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC is an important partner for Twitter and our industry peers. When we are made aware of content depicting or promoting child sexual exploitation, including links to images or content or third party sites where this content can be accessed, the material is removed without further notice and reported to NCMEC. We also partner with nonprofits dedicated to child protection across the globe. In addition to our important relationship with NCMEC, Twitter is an active member of the Technology Coalition. This industry-led non-profit organization strives to eradicate child sexual exploitation by mentoring emerging or established companies, sharing trends and best-practices across industry, and facilitating technological solutions across the ecosystem.

In addition, Twitter is part of the Global Internet Forum to Counter Terrorism, which brings together industry, government, civil society, and academia to share information and collaborate to counter terrorist or extremist content online. Through the GIFCT, we have assembled a shared industry database of “hashes" or digital “fingerprints" for violent terrorist propaganda that spans more than 100,000 hashes. The database allows a company that discovers terrorist content on one of its sites to create a digital fingerprint and share it with the other companies in the forum, who can then use those hashes to identify such content on their services or platforms, review against their respective policies and individual rules, and remove matching content as appropriate or block extremist content before it is posted.

We have also begun to work with a small group of companies to test a new collaborative system to share URLs. Because Twitter does not allow files other than photos or short videos to be uploaded, one of the behaviors we saw from those seeking to promote terrorism was to post links to other services where people could access files, longer videos, PDFs, and other materials. Our pilot system allows us to alert other companies when we removed an account or Tweet that linked to material that promoted terrorism hosted on their service. This information sharing ensures the hosting companies can monitor and track similar behavior, taking enforcement action pursuant with their individual policies. This is not a high-tech approach, but it is simple and effective, recognizing the resource constraints of smaller companies.

Furthermore, in order to safeguard the conversation regarding the 2020 U.S. election, we have critical partnerships with leaders in civic tech, industry, and government organizations, such as the National Association of Secretaries of State, National Association of State Election Directors, Department of Homeland Security, Federal Bureau of Investigation, Department of Justice, Office of the Director of National Intelligence, and elections officials across the country. We also have partnerships with news organizations, civil society, and others, which have been instrumental in informing policies and helping to identify potential threats regarding the integrity of the election conversation occurring on Twitter.

Questions from Senator Blumenthal

6. Since Joe Biden was declared the President-elect, Twitter has scaled its content moderation. However, President Trump routinely flouts Twitter's policies, hourly seeking to delegitimize the election. There is a real threat of violence, and these unfounded allegations are corrosive to our democracy

a. Under what conditions would you return to preventing a viewer from seeing the President's misinformation about the election results unless the user affirmatively clicks "view" on a warning label?

b. Under what conditions would you return to preventing a user from commenting on or retweeting the President's misinformation about the election results?

In October 2020, we clarified our civic integrity policy to provide more information about our efforts to safeguard the public conversation against false claims of victory in the 2020 U.S. election. Applying warnings to premature claims of victory or victory claims that differed from official sources was always intended to be a temporary measure designed to guard against claims of victory when the election outcome was still being determined and the risk of harm was most acute. Once the race was called by official sources and the outcome was widely disseminated, we determined that the risk associated with false claims of victory in the Presidential race significantly decreased and that warnings were no longer necessary to safeguard the public conversation.

Questions from Senator Booker

1. Social media platforms, including Twitter, have a responsibility to stem the flow of election misinformation on their platforms. I believe it is possible for platforms like Twitter to ensure Americans' freedom to speak out while protecting the legitimacy of our democratic process and the public's safety.

a. Has Twitter considered implementing viral circuit breakers as proposed by Professor Ellen Goodman and the Center for American Progress, where social media platforms would design a pause in the algorithmic amplification of fast-growing content about the election until content moderators can conduct an effective review for accuracy? Do you think this would be an effective tool in combatting the flow of misinformation on social media?

b. Has Twitter considered instituting a short delay on content from specific high-reach accounts to allow for human review, just as live network TV institutes a short delay to prevent unacceptable content from airing? Do you think this would be an effective tool in combatting the flow of misinformation on social media?

c. Will Twitter commit to hiding false and misleading content that baselessly delegitimizes our democratic process—content designed to sow doubt and division— behind a click-through warning label? Will Twitter commit to ensuring that its algorithm does not amplify such content?

Twitter has taken numerous steps to combat the spread of misinformation. We have heard from the people who use Twitter that we should not determine the truthfulness of Tweets and we should provide context to help people make up their own minds in cases where the substance of a Tweet is disputed. When we label Tweets, we link to Twitter conversation that shows three things for context: (1) factual statements; (2) counterpoint opinions and perspectives; and (3) ongoing public conversation around the issue. We will only add descriptive text that is reflective of the existing public conversation to let people determine their own viewpoints. In addition, we will reduce the visibility of labeled Tweets, meaning we will not amplify the Tweets on a number of surfaces across Twitter. We also alert people with a warning in cases where they seek to share a Tweet that has been labeled for misinformation, and in some cases disable engagement altogether. This has helped us to combat the potential spread of misinformation on the platform.

While we do not currently institute a short delay on content from high-reach accounts and have not instituted viral circuit breakers, we continue to study and refine our approach to addressing

harms associated with misinformation. We look forward to continuing the conversation with your office about additional steps we can take to address harmful misinformation.

3. What steps have you taken to modify Twitter's algorithms to ensure that blatantly false election disinformation posted by election officials that receives high levels of interaction isn't amplified?

In cases where a label or interstitial is applied, we take steps to reduce the visibility of Tweets, meaning we will not amplify the Tweets on a number of surfaces across Twitter. We may also remove the ability for people to retweet or like the Tweet.

8. President Trump is spreading dangerous misinformation about our electoral process on your platforms right now. What specific lessons have you learned since Election Day? And what concrete steps has Twitter taken to enhance its enforcement policies regarding election disinformation since Election Day?

Our efforts to safeguard the conversation on Twitter regarding the 2020 U.S. election are ongoing and we continue to apply labels, warnings, and additional restrictions to Tweets that included potentially misleading information about the election. We continue to assess the impact of our enforcement actions, but an initial examination of our efforts from October 27th to November 11th has found: ● Approximately 300,000 Tweets have been labeled under our Civic Integrity Policy for content that was disputed and potentially misleading. These represent 0.2% of all US election-related Tweets sent during this time period;

● 456 of those Tweets were also covered by a warning message and had engagement features limited (Tweets could be Quote Tweeted but not Retweeted, replied to, or liked);

● Approximately 74% of the people who viewed those Tweets saw them after we applied a label or warning message; and

● There was an estimated 29% decrease in Quote Tweets of these labeled Tweets due in part to a prompt that warned people prior to sharing.

9. At noon on January 20, Donald Trump will no longer be President of the United States. If he continues to spread election misinformation in the future, will Twitter treat Donald Trump's tweets differently—as an ex-President—from how the platform does now?

We assess reported Tweets from world leaders against the Twitter Rules, which are designed to ensure people can participate in the public conversation freely and safely. We take enforcement action for any account on our service that involves the promotion of terrorism; clear and direct threats of violence against an individual; posting of private information; posting or sharing intimate photos or videos of someone produced or distributed without their content; engaging in behaviors related to child sexual exploitation; engaging in violations of the copyright policy, and encouraging or promoting self-harm. Direct interactions with fellow public figures, comments on political issues of the day, or foreign policy saber-rattling on economic or military issues are generally not in violation of these Twitter Rules

In cases involving a world leader, we will err on the side of leaving the content up if there is a clear public interest in doing so. In such cases, we may place the violative content behind a warning notice that provides context about the violation and allows people to click through should they wish to see the content. Twitter's world leader policy no longer applies when the account in question is no longer a world leader.

10. On November 10, President Trump issued a baseless tweet falsely claiming that an election technology company had "DELETED" millions of his votes and had "SWITCHED" hundreds of thousands more. In fact, a group of federal and state officials responsible for election cybersecurity issued a statement debunking President Trump's claims. "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised," they wrote, adding that "[t]he November 3rd election was the most secure in American history."

a. Is Twitter aware of any evidence to suggest that any election security company deleted millions of Trump votes nationwide?

b. Do you think baseless claims about election fraud are harmful to our democracy?

c. When President Trump posted similarly outrageous tweets during the week of the election, Twitter had hidden those tweets behind a warning label, which had the effect of

reducing how many users were exposed to this false and misleading information. Why was this more recent tweet by President Trump—spreading outrageous falsehoods about the 2020 election—treated differently?

Twitter does not have additional information related to the election security company referenced, beyond what has been publicly reported and shared by government sources. As the response to Question 2 details, in 2020, we updated our civic integrity policy to better safeguard the public conversation around critical civic processes, like the election and census. This policy permits us to take action in cases where individuals make claims that could undermine public confidence in the election, including unverified information about election rigging, ballot tampering, vote tallying, or certification of election results

With regards to the specific Tweet referenced in (c), it was posted on November 12, 2020 and labeled pursuant to Twitter's civic integrity policy.

11. On November 15, President Trump tweeted, "I WON THE ELECTION!" This blatant election misinformation was liked and retweeted hundreds of thousands of times. This and other similar tweets by President Trump were false declarations of victory aimed at undermining the integrity of our electoral process. Why did Twitter decide not to hide this disinformation behind a warning label, as it did for some earlier tweets?

In October 2020, we clarified our civic integrity policy to provide more information about our efforts to safeguard the public conversation against false claims of victory in the 2020 U.S. election. Applying labels and warnings to premature claims of victory or victory claims that differed from official sources was always intended to be a temporary measure designed to guard against claims of victory when the election outcome was still being determined and the risk of harm was most acute. Once the race was called by official sources and the outcome was widely disseminated, we determined that the risk associated with false claims of victory in the Presidential race significantly decreased and that warnings were no longer necessary to safeguard the public conversation.

Questions from Senator Coons

6. In the coming months, it is likely that extensive new information about COVID-19 vaccine candidates will become available. Unfortunately, misinformation about vaccines abounds, and the World Health Organization named resulting vaccine hesitancy one of the top ten threats to global health in 2019. In addition, a recent study found that social media users exposed to content on certain vaccines were more likely to grow misinformed over time than were consumers of traditional media.

a. Is Twitter proactively engaged in planning efforts to address misinformation about emerging COVID-19 vaccines on its platforms?

b. If so, how does Twitter plan to assess the accuracy of information about these vaccines?

c. Has Twitter partnered with (or will Twitter partner with) fact checkers with relevant training and expertise to address misinformation about COVID-19 vaccines?

d. How will Twitter handle vaccine-related content deemed valid when posted but which more recent guidance or consensus suggests is misleading or inaccurate?

e. How will Twitter engage public health, immunology, and other related experts to identify and contextualize content that is incomplete or misleading?

The public conversation occurring on Twitter is critically important during this unprecedented public health emergency. With a critical mass of expert organizations, official government accounts, health professionals, and epidemiologists on our service, our goal is to elevate and amplify authoritative health information as far as possible. To address this global pandemic, on March 16, 2020, we announced new enforcement guidance, broadening our definition of harm to address, specifically, content related to COVID-19 that goes directly against guidance from authoritative sources of global and local public health information. We require individuals to remove violative Tweets in a variety of contexts with the goal of preventing offline harm. Additionally, we are currently engaged in an effort launched by the Office of the U.S. Chief Technology Officer under President Trump in which we are coordinating with our industry peers to provide timely, credible information about COVID-19 via our respective platforms. This working group also seeks to address misinformation by sharing emerging trends and best practices.

In addition, in December 2020, we updated our policy approach to misleading information about COVID-19. Beginning December 21, we may require people to remove Tweets which advance harmful false or misleading narratives about COVID-19 vaccinations, including:

- False claims that suggest immunizations and vaccines are used to intentionally cause harm to or control populations, including statements about vaccines that invoke a deliberate conspiracy;
- False claims which have been widely debunked about the adverse impacts or effects of receiving vaccinations; or
- False claims that COVID-19 is not real or not serious, and therefore that vaccinations are unnecessary.

Starting in early 2021, we may label or place a warning on Tweets that advance unsubstantiated rumors, disputed claims, as well as incomplete or out-of-context information about vaccines. Tweets that are labeled under this expanded guidance may link to authoritative public health information or the Twitter Rules to provide people with additional context and authoritative information about COVID-19. We will enforce this policy in close consultation with local, national and global public health authorities around the world, and will strive to be iterative and transparent in our approach.

Questions from Senator Durbin

2. In their sobering book "How Democracies Die," authors Steven Levitsky and Daniel Ziblatt make the following observation:

"Under President Trump, America has been defining political deviancy down. The president's routine use of personal insult, bullying, lying, and cheating has, inevitably, helped to normalize such practices. Trump's tweets may trigger outrage from the media, Democrats, and some Republicans, but the effectiveness of their responses is limited by the sheer quantity of violations. As [Senator Daniel Patrick Moynihan] observed [in 1993], in the face of widespread deviance, we become overwhelmed and then desensitized. We grow accustomed to what we previously thought to be scandalous. Furthermore, Trump's deviance has been tolerated by the Republican Party, which has helped make it acceptable to much of the Republican electorate."

Mr. Dorsey, I know that Twitter was not conceived as a medium for desensitizing Americans to political deviancy. But President Trump's tweets have had that effect, with serious consequences to our democratic institutions. What is your reaction to the authors' discussion of the normalization of personal insults, bullying, lying, and cheating that has been accelerated through President Trump's tweets?

We assess reported Tweets from world leaders, including President Trump, against the Twitter Rules. In response to violations of the Twitter Rules, we have taken action on a variety of Tweets posted by President Trump, including labeling Tweets or placing them behind an interstitial and limiting amplification. Importantly, we believe there is a value in keeping the content available on our service. There is a public interest in enabling the people to be informed and engage directly with their elected leaders.

While Twitter has a responsibility to safeguard the integrity of the public conversation, we recognize that we are only one part of the broader ecosystem that impacts the broader public discourse. The internet has lowered traditional media barriers to entry for all voices, allowing for unprecedented discourse and community building across the political and socio-economic spectrum. We are happy to work with Congress on efforts to increase civic resilience to better safeguard against harmful misinformation and other concerning behavior.

Questions from Senator Hirono

2. Section 230(c)(1) of the Communications Decency Act currently grants platforms like yours broad immunity for content posted by third parties, even if platforms have knowledge of the content, promote the content, or profit off the content. This immunity applies regardless of platform's size, resources, or efforts to moderate content.

a. Do you believe that all internet platforms should receive the same degree of immunity under Section 230(c)(1) regardless of their size and resources?

b. Do you believe that all internet platforms should receive the same degree of immunity under Section 230(c)(1) regardless of whether, and to what extent, they moderate content?

c. Would you support legislation that required platforms to earn their immunity under Section 230(c)(1) by conditioning immunity on meeting a minimum standard of care?

Section 230 is the Internet's most important law for free speech and safety. Weakening Section 230 protections will remove critical speech from the Internet. We must ensure that all voices can be heard, and we continue to make improvements to our service so that everyone feels safe participating in the public conversation—whether they are speaking or simply listening. The protections offered by Section 230 help us achieve this important objective. Eroding the foundation of Section 230 could collapse how we communicate on the Internet, leaving only a small number of giant and well-funded technology companies. We should also be mindful that undermining Section 230 will result in far more removal of online speech and impose severe limitations on our collective ability to address harmful content and protect people online

As explained in more detail in our written testimony, we do not believe that the solution to concerns raised about content moderation is to eliminate Section 230 liability protections. Instead, we believe the solution should be focused on enhancing transparency, procedural fairness, privacy, and algorithmic choice, which can be achieved through additions to Section 230, industry-wide self-regulation best practices, or additional legislative frameworks.

Questions from Senator Leahy

2. The label used by Twitter to describe the President's election-related tweets states that his claims are disputed, or that other sources called the election differently. In fact, many of these tweets are demonstrably, factually false. To this day, the President is absurdly claiming he won the election. When we know a tweet on your platform will be seen by millions and is objectively false, why not simply label it as "false?

We have heard from the people who use Twitter that we should not determine the truthfulness of Tweets and we should provide context to help people make up their own minds in cases where the substance of a Tweet is disputed. Consistent with this feedback from our customers, we have expanded our enforcement options to allow us to label misinformation related to manipulated media, COVID-19, and civic integrity. When we label Tweets, we link to Twitter conversation that shows three things for context: (1) factual statements; (2) counterpoint opinions and perspectives; and (3) ongoing public conversation around the issue.

EXHIBIT B

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Chairman Frank Pallone, Jr.

Hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"

March 25, 2021

We are here today because the spread of disinformation and extremism has been growing online, particularly on social media, where there are little to no guardrails in place to stop it. And unfortunately, this disinformation and extremism doesn't just stay online. It has real world, often dangerous and even violent consequences. The time has come to hold online platforms accountable for their part in the rise of disinformation and extremism.

According to a survey conducted by Pew earlier this month, 30 percent of Americans are still hesitant or simply do not want to take the COVID-19 vaccine. On January 6, our Nation's Capitol was violently attacked. This month, Homeland Security Secretary Mayorkas identified domestic violent extremism as the "greatest threat" to the United States. And crimes against Asian Americans have risen by nearly 150 percent since the beginning of the COVID-19 pandemic.

Each of these controversies and crimes have been accelerated and amplified on social media platforms through misinformation campaigns, the spread of hate speech, and the proliferation of conspiracy theories.

Five years ago, during the 2016 Presidential elections, Facebook, Google, and Twitter were warned about – but simply ignored – their platforms' role in spreading disinformation. Since then, the warnings have continued, but the problem has only gotten worse. Only after public outrage and pressure, did these companies make inadequate attempts to appease critics and lawmakers. But despite the public rebuke, Wall Street continued to reward the companies' strategy to promote misinformation and disinformation by driving their stock prices even higher.

And now, despite repeated promises to seriously tackle this crisis, Facebook, Google, and Twitter instead routinely make minor changes to their policies in response to the public relations crisis of the day. They will change some underlying internal policy that may or may not be related to the problem. But that's it. The underlying problem remains.

It is now painfully clear that neither the market nor public pressure will force these social media companies to take the aggressive action they need to take to eliminate disinformation and extremism from their platforms. And, therefore, it is time for Congress and this Committee to legislate and realign these companies' incentives to effectively deal with disinformation and extremism.

Today, our laws give these companies, and their leaders, a blank check to do nothing. Rather than limit the spread of disinformation, Facebook, Google, and Twitter have created business models that exploit the human brain's preference for divisive content to get Americans hooked on their platform, at the expense of the public interest. It isn't just that social media companies are allowing disinformation to spread – it's that, in many cases, they are actively amplifying and spreading it themselves. Fines, to the extent they are levied at all, have simply become the cost of doing business.

The dirty truth is that they are relying on algorithms to purposefully promote conspiratorial, divisive, or extremist content so they can rake in the ad dollars. This is because the more outrageous and extremist the content, the more engagement and views these companies get from their users. More views equal more money.

It's crucial to understand that these companies aren't just mere bystanders – they are playing an active role in the meteoric rise of disinformation and extremism.

So when a company is actually promoting this harmful content, I question whether existing liability protections should apply.

Members on this Committee have suggested legislative solutions and introduced bills. The Committee is going to consider all these options so that we can finally align the interests of these companies with the interests of the public and hold the platforms, and their CEOs, accountable when they stray.

That is why you are here today, Mr. Zuckerberg, Mr. Pichai, and Mr. Dorsey. You have failed to meaningfully change after your platforms played a role in fomenting insurrection, in abetting the spread of COVID-19, and trampling Americans civil rights.

And while it may be true that some bad actors will shout fire in a crowded theater, by promoting harmful content, your platforms are handing them a megaphone to be heard in every theater across the country and the world. Your business model itself has become the problem.

The time for self-regulation is over. It is time we legislate to hold you accountable. With that, I yield back.

EXHIBIT C

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Communications and Technology Chairman Mike Doyle

Hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"

March 25, 2021

Our nation is drowning in disinformation driven by social media. Platforms that were once used to share photos of kids with grandparents are all too often havens of hate, harassment, and division.

The way I see it, there are two faces to each of your platforms. Facebook has the family and friends neighborhood but it is right next to the one where there is a white nationalist rally every day.

YouTube is a place where people share quirky videos, but down the street, anti-vaxxers, covid deniers, QAnon supporters, and flat earthers are sharing videos. Twitter allows you to bring friends and celebrities into your home, but also holocaust deniers, terrorists and worse.

Now, it would be one thing if every user chose where to go organically, but almost everything is scripted on social media platforms. Facebook recognizes anti-social tendencies in one user and invites them to visit the white nationalists.

YouTube sees another user is interested in COVID-19 and auto-starts an anti-vax video. On Twitter a user following the trending conversation, never knowing it is driven by bots and coordinated disinformation networks run by foreign agents.

Your platforms have changed how people across the planet - communicate, connect, learn, and stay informed.

The power of this technology is awesome and terrifying - and each of you has failed to protect your users and the world from the worst consequences of your creations.

This is the first time the three of you have appeared before Congress since the deadly attack on the Capitol on January 6th. That event was not just an attack on our Democracy and our electoral process, but an attack on every member of this Committee and in the Congress.

Many of us were on the House floor and in the Capitol when that attack occurred and we were forced to stop our work of certifying the election - and retreat to safety - some of us wearing gas masks and fearing for our lives.

We fled as a mob desecrated the Capitol, the House floor, and our democratic process. People died that day, and hundreds were seriously injured.

That attack and the movement that motivated it started and was nourished on your platforms. Your platforms suggested groups for people to join, videos they should view, and posts they should like - driving this movement forward with terrifying speed and efficiency.

FBI documents show that many of these individuals used your platforms to plan, recruit, and execute this attack.

According to independent research, users on Facebook were exposed 1.1 billion times to misinformation related to the election last year alone - despite changes to your policies and claims that you removed election misinformation.

Our nation is in the middle of a terrible pandemic. Nearly five hundred and fifty thousand Americans have lost their lives to this deadly disease - more than any other country on the planet. An independent study found that on Facebook alone, users across five countries, including the United States, were exposed to COVID disinformation an estimated 3.8 billion times - again despite claims of fixes and reforms.

And now as the Biden Administration is working to implement the American Rescue Plan and get vaccines in people's arms, we are faced with waves of disinformation on social media about the safety and efficacy of these shots.

These vaccines are the best chance we have to fight this virus, and the content that your websites are still promoting, still recommending, and still sharing - is one of the biggest reasons people are refusing the vaccine.

And things haven't changed – my staff found content on YouTube telling people not to get vaccines and was recommended similar videos.

The same was true on Instagram, where it was not only easy to find vaccine disinformation - but the platform recommended similar posts. The same thing happened on Facebook except they also had anti-vax groups to suggest as well.

Twitter was no different, if you go to any of the super spreader accounts that remain up despite policies meant to curb anti-vax content, you'll see this content.

You **can** take down this content, you **can** reduce division, you **can** fix this - but you choose not to.

We saw your platforms remove ISIS terrorist content; we saw you tamp down on COVID misinformation at the beginning of the pandemic; we have seen disinformation drop when you have promoted reliable news sources and removed serial disinformation super spreaders from your platforms.

You have the means, but time after time, you are picking engagement and profit over the health and safety of your users, our nation, and our democracy.

These are serious issues, and to be honest - it seems like you all just shrug off billion-dollar fines. Your companies need to be held accountable - we need rules, regulations, technical experts in government, and audit authority of your technologies. Ours is the committee of jurisdiction, and we will legislate to stop this. The stakes are simply too high.

EXHIBIT D

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Consumer Protection and Commerce Chair Janice D. Schakowsky

Hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation"

March 25, 2021

I want to welcome our witnesses and thank them for coming. It is not an exaggeration to say that your companies have fundamentally and permanently transformed our very culture: and our understand of the world.

Much of this is for the good, but it is also true that our country, our democracy, even our understanding of what is truth, has been harmed by the proliferation of disinformation, misinformation, and extremism, all of which has deeply divided us.

What our witnesses need to take away from this hearing is that self-regulation has come to the end of its road, and that this democratically elected body is prepared to move forward with legislation and regulation.

The regulation we seek should not attempt to limit Constitutionally protected free speech, but it must hold platforms accountable when they are used to incite violence and hatred—— or as in the case of the Covid pandemic – spread misinformation that costs thousands of lives.

All three companies here today run platforms that are hotbeds of misinformation and disinformation.

Despite all the promises and new policies to match, disinformation was rampant in the 2020 election -- especially targeting vulnerable communities.

For example, Spanish language ads run by the Trump campaign falsely claimed President Biden was endorsed by Venezuelan President Maduro. The spread of disinformation fed upon itself until it came to a head in the historic assault on our Capitol and our democracy on January 6th, which cost 5 lives.

The lives lost to the Insurrection were not the first casualties of these platforms' failures, nor are they the worst. In 2018, Facebook admitted a genocide of the Rohingya people in Myanmar was planned and executed on Facebook.

2020 saw the rise of coronavirus disinformation on Facebook's platforms including the propaganda film "Plandemic." This film got 1.8 million views and 150,000 shares before it was removed by Facebook.1

Disinformation like Plandemic made people skeptical of the need for vaccines and almost certainly contributed to the horrible loss of life during the pandemic.

Disinformation also hops platforms to spread virally across the internet. Plandemic was first posted on YouTube before taking off on Facebook, Instagram, and Twitter. Misinformation regarding the election dropped by 73% across social media platforms after Twitter permanently suspended Trump as well as accounts tied to the Capitol Insurrection and QAnon.2 The question is, what took so long?

The witnesses here today have demonstrated time and again that promises to self-regulate don't work. They must be held accountable for allowing disinformation and misinformation to spread across their platforms, infect our public discourse, and threaten our democracy.

That's why I'll be introducing the Online Consumer Protection Act, which I hope will earn bipartisan support.

Thank you, and I yield back.

EXHIBIT E

COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

March 22, 2021

To: **Subcommittee on Communications and Technology and Subcommittee on Consumer Protection and Commerce Members and Staff**

Fr: **Committee on Energy and Commerce Staff**

Re: **Hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Disinformation"**

On **Thursday, March 25, 2021, at 12 p.m. via Cisco Webex online video conferencing**, the Subcommittee on Communications and Technology and the Subcommittee on Consumer Protection and Commerce will hold a joint hearing entitled, "Disinformation Nation: Social Media's Role in Promoting Extremism and Disinformation."

I. THE ROLE OF SOCIAL MEDIA PLATFORMS IN PROMOTING MISINFORMATION AND EXTREMIST CONTENT

A. Background

Facebook, Google, and Twitter operate some of the largest and most influential online social media platforms reaching billions of users across the globe. As a result, they are among the largest platforms for the dissemination of misinformation and extremist content.[1] These platforms maximize their reach—and advertising dollars—by using algorithms or other technologies to promote content and make content recommendations that increase user engagement.[2] Users of these platforms often engage more with questionable or provocative content, thus the algorithms often elevate or amplify disinformation and extremist content.[3] Facebook, Google, and Twitter also have access to vast swaths of user data that allows them to microtarget content to users who would be more susceptible to disinformation and extremist content.[4]

---

[1] *See* NYU Stern Center For Business And Human Rights, *Tackling Domestic Disinformation: What The Social Media Companies Need To Do* (Apr. 3, 2019).

[2] *See id*.

[3] *See id*.

[4] *See How Data Privacy Laws Can Fight Fake News*, Just Security (Aug. 15, 2019).

B. The Spread and Consequences of Misinformation and Extremist Content

Facebook, Google, and Twitter have long come under fire for their role in the dissemination and amplification of misinformation and extremist content. For instance, since the beginning of the coronavirus disease of 2019 (COVID-19) pandemic, all three platforms have spread substantial amounts of misinformation about COVID-19.[5] At the outset of the COVID-19 pandemic, disinformation regarding the severity of the virus and the effectiveness of alleged cures for COVID-19 was widespread.[6] More recently, COVID-19 disinformation has misrepresented the safety and efficacy of COVID-19 vaccines.[7]

Facebook, Google, and Twitter have also been distributors for years of election disinformation that appeared to be intended either to improperly influence or undermine the outcomes of free and fair elections.[8] During the November 2016 election, social media platforms were used by foreign governments to disseminate information to manipulate public opinion.[9] This trend continued during and after the November 2020 election, often fomented by domestic actors, with rampant disinformation about voter fraud, defective voting machines, and premature declarations of victory.[10]

Additionally, Facebook executives were repeatedly warned that extremist content was thriving on their platform, and that Facebook's own algorithms and recommendation tools were responsible for the appeal of extremist groups and divisive content.[11] Similarly, since 2015, videos from extremists have proliferated on YouTube; and YouTube's algorithm often guides

---

[5] *Democratic Senators Urge Facebook, Google and Twitter to Crack Down on Vaccine Misinformation*, CNBC (Jan. 25, 2021); *Surge of Virus Misinformation Stumps Facebook and Twitter*, New York Times (Mar. 8, 2020).

[6] *Id.*

[7] '*We Are Talking About People's Lives': Dire Warnings of Public Health Crisis as COVID-19 Misinformation Rages*, USA Today (Dec. 9, 2020); *Misinformation Messengers Pivot from Election Fraud to Peddling Vaccine Conspiracy Theories,* New York Times (Dec. 16, 2020); *Normalization of Vaccine Misinformation on Social Media Amid COVID 'a Huge problem*,' ABC News (Dec. 10, 2020); *COVID Vaccine: Disappearing Needles and Other Rumors Debunked*, BBC News (Dec. 20, 2020).

[8] *Election 2020: Facebook, Twitter And YouTube Wrestle With Misinformation*, CNET (Nov. 11, 2020); NYU Stern Center for Business and Human Rights, *Disinformation and the 2020 Election: How the Social Media Industry Should Prepare* (Sept. 1, 2019).

[9] *The Propaganda Tools Used by Russians to Influence the 2016 Election*, New York Times (Feb. 16, 2018).

[10] *'Not A Whole Lot Of Innovation': 2020 Election Misinformation Was Quite Predictable, Experts Say*, USA Today (Nov. 17, 2021); *Did Social Media Actually Counter Election Misinformation?*, Associated Press, (Nov. 4, 2020).

[11] *Facebook Executives Shut Down Efforts To Make The Site Less Divisive*, Wall Street Journal (May 26, 2020); *Facebook Knew Calls For Violence Plagued 'Groups,' Now Plans Overhaul*, Wall Street Journal (Jan. 31, 2020).

users from more innocuous or alternative content to more fringe channels and videos.[12] Twitter has been criticized for being slow to stop white nationalists from organizing, fundraising, recruiting and spreading propaganda on Twitter.[13]

The consequences of disinformation and extremist content on these platforms are apparent. Many experts agree that disinformation about COVID-19 has greatly intensified an already deadly public health crisis.[14] Experts also acknowledge that misinformation about the 2020 presidential election and extremist content has further divided the nation and provoked an insurrection.[15]

C. Facebook, Google, and Twitter's Response to Misinformation and Extremist Content

All three platforms have a policy against demonstrably false COVID-19 information or COVID-19 misinformation that can cause harm.[16] Facebook and Twitter also demote or label certain misinformation, such as misinformation about social and political issues.[17]

In September 2020, Facebook adopted new policies related to the November election such as banning political advertisements and labeling allegations of election fraud.[18] After the January 6, 2021 U.S. Capitol riots, Facebook began removing disinformation that could lead to further violence.[19] Last month, Facebook updated its policies on COVID-19 misinformation from initially removing false information "that could lead to imminent physical harm" to banning misinformation about COVID-19 and threatening to ban users, groups, or pages that repeatedly spread misinformation.[20]

In October 2020, YouTube announced it would remove videos containing misinformation about COVID-19 vaccines, expanding on its prohibition of COVID-19 misinformation that

---

[12] Cornell University, *Auditing Radicalization Pathways On YouTube* (Dec. 4, 2019).

[13] *Twitter Suspends More Than 50 White Nationalist Accounts*, NBC News (July 10, 2020); *Twitter Still Has A White Nationalist Problem*, HuffPost (May 30, 2019).

[14] The Union of Concerned Scientists, *We Just Witnessed the Dangers of the Autocratic Disinformation Playbook* (Jan. 8, 2021) (blog.ucsusa.org/genna-reed/dangers-of-autocratic-disinformation-playbook).

[15] *Id*.

[16] *On Social Media, Only Some Lies Are Against The Rules*, Consumer Reports (Aug. 13, 2020).

[17] *Id*.

[18] Facebook, *New Steps to Protect the US Elections* (Sept. 3, 2020) (press release).

[19] Facebook, *Our Preparations Ahead of Inauguration Day* (Jan. 11, 2021) (press release).

[20] Facebook, *An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19* (Feb. 8, 2021) (press release).

contradicted local health authorities or the World Health Organization.[21] In December 2020, YouTube announced it would begin removing content that falsely alleged widespread election fraud, but that policy would not apply to videos uploaded prior to the announcement.[22] After the U.S. Capitol riots, YouTube announced that it would suspend accounts that promoted videos of false allegations about the 2020 presidential election.[23]

In advance of the November 2020 election, Twitter expanded the use of its warning labels to limit the spread of election misinformation.[24] In December 2020, Twitter announced it would label misinformation about COVID-19 vaccines.

These platforms often ramp up their efforts against misinformation and extremist content in response to social and political pressure.[25] Despite these efforts, recent studies have found that COVID-19 misinformation and extremist content continue to thrive on these platforms.[26]

II. WITNESSES

The following witnesses have been invited to testify:

Mark Zuckerberg
Chairman and Chief Executive Officer
Facebook

Sundar Pichai
Chief Executive Officer
Google

---

[21] *YouTube Bans Covid-19 Vaccine Misinformation*, Forbes (Oct. 14, 2020); *On Social Media, Only Some Lies Are Against the Rules*, Consumer Reports (Aug. 13, 2020).

[22] YouTube Official Blog, *Supporting The 2020 U.S. Election* (Dec. 9, 2020) (blog.youtube/news-and-events/supporting-the-2020-us-election/).

[23] *YouTube Will Start Penalizing Channels That Post Election Misinformation*, TechCrunch (Jan. 7, 2021).

[24] Twitter Blog, *Additional Steps We're Taking Ahead of the 2020 US Election* (Oct. 9, 2020) (blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html).

[25] *See The Technology 202: Democrats Ratchet Up Pressure on Silicon Valley to Tackle Vaccine Misinformation*, Washington Post (Jan. 26, 2021); *Social Media Platforms Face A Reckoning Over Hate Speech*, Associated Press (June 29, 2020); *EU Piles Pressure On Social Media Over Fake News*, Reuters (Apr. 26, 2018).

[26] Cybersecurity for Democracy, *Far-Right News Sources On Facebook More Engaging* (Mar. 3, 2021); Pew Research Center, *How Americans Navigated the News in 2020: A Tumultuous Year in Review* (Feb. 22, 2021); Anti-Defamation League, *Exposure to Alternative & Extremist Content on YouTube* (Feb.12, 2021); The German Marshall Fund, *Engagement With Deceptive Outlets Higher on Facebook Today than Run-Up to 2016 Election* (Oct. 12, 2020).

Jack Dorsey
Chief Executive Officer
Twitter